ICT and employer-employee power dynamics

Cuijpers, C.M.K.C.

Published in:
Yonsei Law Journal

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

<연구논문>

정보통신기술과 사용자 - 근로자간의 역학관계*

- 정보통신기술에 의한 근로자 감시 및 근로자의 위치추적에 있어서 사업장 내 프라이버시에 대한 미국과 네덜란드의 비교법적 관점의 연구 -

Colette Cuijpers** · 이재용***

◈ 목 차 ◈

---

* [역주] 논문의 원제목은 ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherland's Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning 이며, 출처는 *The John Marshall Journal of Computer & Information Law (Winter, 2007)*이다. 본 논문은 저자(C.M.K.C.Cuijpers@uvt.nl)의 동의를 얻어 번역하였으며, 일부 각주와 유효하지 않은 인터넷 링크 등을 역자가 삭제하거나 수정한 부분이 있음을 밝혀둔다.

** 네덜란드 Tilburg University Law School 교수. 노동법, 저작권법, 프라이버시법 등의 권위자로 현재는 TILT(Tilburg Institute for Law, Technology, and Society)에서 노동법, 소비자법법의 영역에서 법, 기술, 힘의 균형 이동에 관해 연구하고 있다. 본 논문도 이러한 연구프로젝트의 일부이다.

*** 법학박사(연세대학교), 숙명여자대학교 법학과 겸임교수, 연세대학교 대학원 강사

Ⅰ. 서설

1. 연구의 주제 및 방법

지난 10년 동안 많은 사업장에서 인터넷과 이메일이 사용되기 시작하였다. 사용자의 입장에서 보면 이 신기술들은 장점도 있으나 그만큼 리스크도 따르게 된다. 특히 이러한 리스크는 근로자들이 이 기술을 사용하는 것과 관련이 있다. 예를 들어 근로자들이 이메일이나 핸드폰을 통해 회사 기밀을 누설함으로써 회사에 금전적인 피해를 줄 수 있다. 아니면 근무시간에 사적인 용도로 인터넷을 사용하는 것 자체도 회사에 금전적인 피해가 된다. 또한, 근로자들이 사내전화나 인터넷을 통하여 외설적이거나 남을 비방하는 글을 올림으로써 회사의 명성에 금이 가게 할 수도 있다. 이러한 리스크를 최소화하기 위해서 사용자는 인터넷이나 이메일을 감시할 수 있는 장비를 설치하기도 한다.[1] 인터넷이나 이메일의 사용과 함께 이를 감시할 수 있는 장비의 설치는 사용자와 근로자간의 관계에 큰 영향을 미치게 된다. 다른 한편으로 정보통신기술(Information and Computer Technology)이 근로자들의 통신범위를 확장함으로써 이들이 더 많은 권리를 가질 수도 있으나 사용자 또한 정보통신기술을 통하여 근로자의 활동을 훨씬 더 손쉽게 감시할 수 있게 됨에 따라 더 많은 권한을 가지게 된다.[2]

정보통신기술이 갖는 이러한 이중적 성격을 감안하여 본 논문은 다음 질문에

---

1) 미국경영자협회(AMA: America Management Association)의 2005년 사업장 전자감시실태조사결과에 따르면 응답기업 중 36%가 근로자의 컴퓨터 사용시간과 내역을 감시하고 있고, 50%는 근로자의 컴퓨터 파일을 열람・저장하고 있으며, 55%는 이메일을 감시하고 있는 것으로 나타났다. Michael Rustad & Sandra R. Paulsson, Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshops: Insights from Europe, *7 U. Pa. J. Lab. & Emp. L. 829 (2005)* [Reginald C. Govan and Freddie Mac, 33rd Annual Institute on Employment Law: Workplace Privacy, 712 PLI/Lit 245 (2004)에서 인용].

2) [역주] 근로자들에 대한 사용자의 감시를 뜻하는 영문표현으로는 'monitoring'과 'surveillance'가 있는데 ILO에서는 'monitoring'은 직무수행 및 결과에 대한 협의의 감시로, 'surveillance'는 사업장내에서 근로자들의 전반적인 근로활동 및 직장생활에 대한 포괄적인 감시활동으로 구별하고 있다(ILO, Conditions of Worker's Privacy, Vol.12, No.3, 1993).

대한 답을 찾는 데 집중할 것이다. 정보통신기술이 사용자와 근로자간의 힘의 균형에 어떠한 영향을 미치는가, 그리고 이러한 힘의 균형의 변동을 규제하는 데 있어 관련 법령이 적절한가? 정보통신은 다양한 면을 가지고 있으며 근무환경에 깊숙이 침투해있기 때문에 본 논문 하나로 모든 분야를 다룰 수는 없을 것이다. 따라서 정보통신이 사용자와 근로자간의 힘의 균형에 대해 분명한 영향을 미치고 있는 두 가지 구체적인 시나리오에 집중하기로 한다. 우선 사업장에서 인터넷과 이메일을 감시하는 데 사용되는 다소 정교한 시스템에 관하여 다루기로 한다. 두 번째 시나리오는 회사 내에서는 물론 회사 밖에서 근로자의 위치를 감시하는 것과 관련된 것이다. 위치추적시스템의 사용은 사용자가 근로자를 감시하는 데 있어 새로운 유행이 되어가고 있다.[3] 이러한 감시수단과 관련하여, 본 논문은 이메일과 인터넷 감시를 규제하는 법령이 같은 방식으로 위치추적시스템에도 적용이 될 수 있을지를 살펴볼 것이며, 이러한 법령의 적용이 사용자와 근로자간의 관계에 있어 어떤 결과를 가져올지를 검토해 볼 것이다. 본 논문에서 언급되는 구체적인 사례들을 통하여 법령 체계와 이러한 체계와 관련된 힘의 균형에 대하여 결론을 내릴 예정이다. 비교법적인 관점에서 미국과 네덜란드의 사례가 다루어질 것이다. 이 두 나라의 법령을 비교해 보는 것은 매우 흥미롭다. 왜냐하면 양국이 사생활과 사생활 관련 규제에 대해 접근하는 방식이 무척 다를 뿐 아니라 노동법의 기본 원칙 및 규정에 있어 큰 차이가 있기 때문이다.[4] 따라서 양국의 비교를 통하여 사용자와 근로자간의 힘의 균형에 있어 정보통신을 활용한 감시와 위치추적이 미치는 영향에 대해 새로운 시각을 가질 수 있을 것이다.

3) Google에서 'GPS Monitoring Employees'를 검색해 보면 관련 서비스의 증가추세를 확인할 수 있다.

4) P. Blok, Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht, Boom Juridische Uitgevers, ch. 3-8 (2002); Antoine Jacobs, Sociale rechten in Amerika, Utrecht: LEMMA BV, 212 (2003); Antoine Jacobs, Labour Law in the Netherlands, Kluwer Law International (2004).

2. 연구의 배경

근로자들이 사적인 용도로 이메일이나 인터넷을 사용하는 경우 리스크가 따르기 때문에 회사는 근로자들의 이메일이나 인터넷 사용을 감시할 동기를 가지게 된다.[5] 근로자들이 이메일이나 인터넷을 사용함으로써 그들의 생산성에 악영향을 미칠 수 있을 뿐 아니라 회사가 법적 책임을 져야 하는 경우도 있으며 특히 회사의 명성에 심각한 타격을 줄 수도 있다.[6]

이러한 이유로 인하여 사용자가 가장 손쉽게 택할 수 있는 해결책은 사업장에서의 개인적인 이메일이나 인터넷 사용을 금하는 것이다. 그러나 연구에 따르면 이를 금하는 경우 근로자들의 사기에 부정적인 영향을 미치게 됨에 따라 오히려 생산성의 저하가 있을 수 있다. 또한 이메일과 인터넷을 개인적으로 사용함으로써 실제 업무 목적으로 이러한 기술을 사용할 수 있는 능력을 향상시킬 수도 있다.[7] 이와 같이 일반적인 업무 활동을 방해하지 않고 개인적인 사용을 방지할 수 있는가 하는 것은 사내 전화를 개인적으로 사용하는 것을 막는 것과 유사하다. 특이한 점은 사내전화의 개인적인 사용은 어느 정도는 용인된다는 것이다. 근로자들이 인터넷이나 이메일을 개인적으로 사용하는 것은 허용하는 대신 사용자는 감시장비를 설치함으로써 인터넷 사용을 억제할 수 있는 방법들을 찾고 있다. 대표적인 예가 영상감시장비, 인터넷감시장비 및 위치추적

5) 이러한 감시는 경영활동에 대한 통제나 생산성, 효율성, 품질 등의 평가처럼 사용자가 일정한 이해관계를 갖는 경우에만 정당화될 수 있다.

6) R. Blanpain & Michelle Colucci, The Impact of the Internet and New Technologies on the Workplace. A Legal Analysis from a Comparative Point of View, The Hague: Kluwer, 14-16 (2002); see also R. Blanpain, On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work, The Hague/London/New York: Kluwer, 44 (2002).

7) Blanpain & Colucci, supra note 6, at 18; see also Jay P. Kesan, Cyber-Working or Cyber-Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace, 54 Fla. Law Rev. 289, 319 (2002); Rustad, supra note 2, at 19; Peter Blackman & Barbara Franklin, Blocking Big Brother: Proposed Law Limits Employer's Right to Snoop, N.Y. L. J., at 5 (1993); Kenneth A. Kovach, The Balance Between Employee Privacy And Employer Interests', 105 Business and Society Review 289, 295 (2000).

시스템이다.[8] 인터넷과 이메일의 개인적인 사용으로 인한 리스크는 이러한 새로운 감시장비의 사용을 정당화한다. 이러한 감시장비는 단순한 생산성 점검 이상의 역할을 하게 된다. 그러나 이러한 사업장 내 감시장비를 포함하여 사용자가 자신의 방식대로 사업을 수행할 수 있는 권리는 근로자의 프라이버시권과 충돌을 일으킬 수 있다. 사용자와 근로자가 갖는 권리 간에 조화를 찾기 위하여 근로자에 대한 감시는 그 범위와 효력에 있어 일정한 제한을 받아야만 할 것이다. 감시를 하다 보면 흔히 순수한 사업 목적이나 회사 자산을 지키는 목적을 넘어설 수 있기 때문이다. 적절한 예방책이 없는 경우 감시나 위치추적시스템을 통하여 사용자는 근로자의 일거수일투족을 파악할 수 있게 된다. 이는 사용자에게 지나친 권한을 부여하게 될 것이다. 본 논문에서는 미국과 네덜란드의 법률이 적절한 예방책이 될 수 있는지를 검토해 보기로 한다.

Ⅱ. 인터넷과 이메일 감시에 대한 미국과 네덜란드 법률의 접근 방식

1. 개요

본 제Ⅱ장에서는 인터넷과 이메일 감시에 있어 미국과 네덜란드 법률의 접근 방식에 있어 공통점과 차이점을 다루게 된다. 이를 위하여 우선 프라이버시권에 있어 양국의 차이점을 검토하게 될 것이다. 아래에서 살펴보는 바와 같이 미국에서는 프라이버시가 시장원리에 의하여 일종의 재산권의 입장에서 다루어지는데 반해 네덜란드에서는 기본적인 인권의 문제로 다루어진다.[9] 관련 문헌이나 법률 및 판례법을 바탕으로 회사에 의한 인터넷과 이메일 감시의 허용 여부 및 허용 정도, 근로자의 프라이버시권을 보장하기 위한 대책에 대한 일반적인 결론을 도출하게 될 것이다.

---

8) Blanpain & Colucci, supra note 6, at 18.

9) See Rustad supra note 2; Blok, P., Het recht op privacy. Een onderzoek naar de betekenis van het begrip ‘privacy’ in het Nederlandse en Amerikaanse recht, Boom Juridische Uitgevers, ch. 3-8 (2002); see also Blanpain, supra note 7, at 95-125, 233-251.

2. 미국의 접근방식[10]

가. 헌법 및 불법행위법

미국에서 사용자에 의한 감시에 대해 근로자가 사용할 수 있는 구제책으로 프라이버시권과 관련된 세 가지[11] 법원(法源, sources of law)을 고려해 볼 수 있다. 부당한 수색과 체포·압수를 금지한 제4차 연방수정헌법(the Fourth Amendment of the Federal Constitution)[12], 전자통신 관련 프라이버시법(the Electronic Communications Privacy Act, 이하 ECPA법)과 사생활침해에 대한 불법행위책임(the privacy tort of intrusion into seclusion)이 바로 그 세 가지 법원이다. 이중 제4차 연방수정헌법과 사생활침해에 대한 불법행위책임에 있어 인터넷과 이메일 감시의 적법성 여부는 당해 근로자가 프라이버시에 대한 정당한 기대(reasonable expectation of privacy)가 있었느냐에 달려 있게 된다.[13] 미국 판례법에 대한 문헌에 따를 경우 사업장 내에서는 프라이버시에 대한 정당한 기대가 결코 있을 수 없다고까지 한다.[14] 만일 프라이버시에 대한 정당한 기대가 있는 경우라 할지라도, 사용자는 직원들에게 인터넷과 이메일 사용이 감시 받고 있다고 고지함으로써 이러한 기대를 효과가 없는 것으로 할 수 있다.[15] 판례법에 의하면 심지어 사용자는 고지 없이도 직원들의 인터넷과 이메

---

10) [역주] 미국의 경우 주마다 법률이 상이한 연방국가라는 특성으로 인해 광범위한 판례법으로부터 지극히 일반적인 결론만이 도출될 수 있다.

11) See Mark Sullivan, Wired, Arnold Vetoes Privacy Bill, Sept. 30, 2004; Karen Eltis, The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Case law in Canada and Israel: Should Others Follow Suit?, 24 Comp. Lab. L. & Pol'y J. 487 (2003); see also Blanpain, supra note 7, at 233-251; Blanpain & Colucci, supra note 7, at 155-157; Kesan, supra note 8; Rustad & Paulsson, supra note 2.

12) 개인은 사용자가 공공기관인 경우에 한해 제4차 수정헌법상의 권리를 주장할 수 있다.

13) *O'Connor v. Ortega, 480 U.S. 709 (1987)*; see also Gellman, R., A General Survey of Video Surveillance Law in the United States, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, Den Haag: T.C.M. Asser press (2005).

14) See e.g. Rustad & Paulsson, supra note 2, at 10.

일 사용을 감시할 수 있다고 한다.[16] 'Smyth v. Pillsbury Co.' 사례에서 법원은 근로자가 사업장에서 사용하는 이메일과 관련하여 어떠한 프라이버시에 대한 기대도 가질 수 없다고 하였다. 왜냐하면 당해 근로자가 사업장에서 제공하는 이메일 계정을 자발적으로 사용하기로 한 순간 정당한 기대가 사라지기 때문이라고 한다.[17] 심지어 사용자가 근로자들에게 모든 이메일 통신의 기밀성을 보장해 주었다 할지라도 감시가 여전히 허용될 수 있다고 한다. 왜냐하면 부적절하거나 직업윤리에 어긋나는 발언이나 이메일 시스템상에서 일어나는 불법적인 활동에 대해 회사가 가지는 이익이 근로자가 가지는 프라이버시에 대한 이익보다 더 중요하기 때문이라고 한다.[18] 결과적으로 사용자가 근로자의 인터넷이나 이메일을 감시하여 사생활이 침해되었다는 이유로 제4차 연방수정헌법이나 사생활의 침해에 대한 불법행위책임을 근거로 소송을 제기한다 할지라도 근로자가 승소할 가능성은 매우 낮다고 할 것이다.[19]

사생활의 침해에 대한 불법행위책임에 있어서는 실제 침해가 성립하기 위해서 충족되어야 할 더 중요한 요건이 있는데, 당해 침해의 정도가 매우 심각해야 한다는 것이다.[20] 사용자가 행하는 인터넷이나 이메일 감시는 신체적인 침해가 없기 때문에 그러한 요건을 충족하기는 사실상 힘들다.[21] 더욱이 제4차 연방수정헌법은 그 적용 대상이 공공 사용자로서 그들의 활동이 '국가 활동(state actions)'으로 간주될 수 있는 경우에만 적용이 가능하다.[22] 또한, '수색(search)'의 정의로 인해 제4차 연방수정헌법의 적용범위가 줄어들게 된다. 'Kyllo v.

15) Robert Fragale Filhot & Mark Jeffery, Information Technology and Workers' Privacy: Notice and Consent, A Comparative Study: Part III: Recurring Questions of Comparative Law, *23 Comp. Lab. L. & Pol'y J. 471, 557-558 (2002).*

16) See *Garrity v. John Hancock Mut. Life Ins. Co., 2002 U.S. Dist. LEXIS 8343* (D. Mass. May 7, 2000).

17) *Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996)*; Kovach, supra note 8, at 294.

18) Id.

19) Filhot, supra note 16, at 560.

20) *Miller v. Natl. Broadcasting Co., 187 Cal. App. 3d 1463 (Cal.App. 2nd Dist. 1986).*

21) Dan Long, The Electronic Workplace, Modrall, Sperling, Roehl, Harris & Sisk, P.A., June 3, 2002.

22) Parry Aftab, Monitoring Law: To Videotape or Not to Videotape. That Is the Question, http://www.aftab.com/videotapinglaw.htm.

United States' 사례에 의하면 정부가 일반적으로 공공에 의하여 사용되지 않는 기술을 활용하여 신체적 침해 없이 사적인 영역에서 정보를 수집한 경우에만 '수색'의 정의에 포섭되게 된다.[23] 따라서 육안이나 흔히 사용되는 시각장비를 활용한 시각 감시(visual surveillance)는 이러한 '수색'에 포함되지 않는다.[24]

'Ortega' 사례에 따르면 프라이버시에 대한 정당한 기대가 있는 경우에만 사용자의 침해의 적절성 여부가 검토된다.[25] 동 사례에서는 사업장에서의 영장 없는 수색의 적법성 여부가 핵심이었는데 법원은 영장을 발급받아야 하는 부담이 수색을 행하는 정부의 목적 달성에 방해가 될 가능성이 있는 경우에만 예외적으로 영장 없는 수색이 적법할 수 있다고 하였다.[26] 또한 법원은 사업장이라는 장소 자체가 이러한 예외성을 충족할 수 있다고 하였다.[27] 더 나아가 법원은 수색의 개시와 직원의 사생활에 대한 침해 정도가 합리성이라는 기준을 충족해야만 한다고 판결하였다.[28] 수사를 위한 수색의 경우 위법행위를 의심할 수 있을 정도의 정당한 이유가 있다면 수색의 개시를 위한 요건은 충족될 수 있을 것이다.[29] 사용되는 수단이 수색의 목적과 합리적으로 관련이 있고 위법행위의 정도를 고려해 보았을 때 지나친 침해가 아니라면 수색의 범위 또한 합리적인 것으로 판정될 수 있다.[30]

위에서 언급한 바와 같이 직원들에게 고지만 한다면 프라이버시에 대한 기대를 제거할 수 있고, 사용자는 원하는 만큼 사생활을 침해할 수 있으며, 사용자의 활동에 대한 법적 책임 또한 발생하지 않을 것이다. 그 근본 이유는 근로자가 프라이버시에 대한 정당한 기대를 가지는 경우에만 사용자의 활동이 정당하

23) *Kyllo v. United States, 533 U.S. 27, 34 (2001).*
24) Peter Caldwell, GPS Technology in Cellular Telephones: Does Florida's Constitutional Privacy Protect Against Electronic Locating Devices?, *11 J. Tech. L. & Pol'y 39, 44 (2006).*
25) *O' Connor v. Ortega, 480 U.S. 709 (1987).*
26) Id.
27) Id.
28) Id.
29) Id.
30) David J. Phillips, Privacy and Data Protection in the Workplace: the U.S. Case, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, 42 (2005).

지 않은 것으로 평가되기 때문이다. 이러한 판결이 합리적인지 여부는 의심스럽다. 사용자가 자신을 감시할 수 있다는 사실을 인지하고 있다 할지라도 사용자의 지나친 감시는 여전히 근로자에게 피해를 줄 수 있다. 경제적이거나 심리적인 피해를 상정해 볼 수 있으며, 사업장과 가정이 점점 더 긴밀한 관계를 맺고 있음을 감안할 때 피해를 입게 될 가능성은 더욱 커진다. 근로자가 사무실에 개인적인 소유물이나 정보를 소지하고 있는 경우를 상정해 볼 수 있다.[31] 혹은 회사 자산이나 정보를 직원의 가정에서 접속하거나 사용하는 경우도 생각해 볼 수 있다. Ernst & Young사의 연례 조사보고서에 따르면 사용자는 핸드폰이나 노트북을 활용하여 휴일에도 직원들에게 연락을 취할 수 있다.[32] 이런 면을 감안할 때 사용자의 활동이 합리적인지 여부는 프라이버시에 대한 정당한 기대와는 별도로 고려되어야 하며 이러한 활동에 대하여 법적인 책임을 지는 것도 가능해야 한다.

결론적으로 미국 법원은 개인적이며 자치적인 사생활에 대한 헌법상 권리를 인정하면서도 개인정보공개에 대한 프라이버시권이라 알려져 있는 개인의 자기정보통제권을 보호하는 데는 매우 인색하다.[33] 불법행위법은 개인정보를 공개하는데 대한 구제책을 마련하고 있다. 그러나 이들은 고용관계에 있어서는 제기능을 발휘하지 못하고 있다. '정보공개(public disclosure)'는 일반 대중에게 정보를 공개하는 것을 의미한다. 회사 경영진과 같이 일정 범위의 사람들만이 접근이 가능한 웹사이트상에 정보를 공개하는 것은 '정보공개'에 해당하지 않는다. 더욱이 고용관계와 관련된 사실의 공개는 개인정보라는 개념 자체에 일반적으로 포섭되지 않는다.[34]

---

31) See Earnest & Young, ICT Borometer, http://www.ict-barometer.nl/rapporten.php.

32) See Id.

33) Caldwell, supra note 25, at 49; see also *Whalen v. Roe, 429 U.S. 589, 605-06 (1977)*; see also Index of /pub/97-98/bill/asm, Number 1323 cfa 19970516, http://info.sen.ca.gov/pub/97-98/bill/asm.

34) Jill Yung, Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should do About It, 36 Seton Hall L. Rev. 163, 192 (2005).

나. 전자통신 관련 프라이버시법(ECPA법)

ECPA법은 전자통신을 감시하는 것과 관련된 보다 구체적인 규정을 담고 있다.[35] 본 법률이 전화, 구두, 전자통신(이메일을 포함하는 것으로 해석됨) 및 저장된 통신 내용을 도청하는 것을 금지하고 있긴 하지만 각종 예외 조항이 본 법률의 효력을 제한하고 있어 고용관계에서는 사실상 효력을 전혀 발휘하지 못하고 있다. 첫 번째로 검토해 볼 예외 조항은 '제공자 예외'(provider exception)이다. 본 예외 조항을 폭넓게 해석할 경우 이메일 통신을 저장할 수 있는 컴퓨터나 네트워크를 보유하고 있는 모든 사기업체는 내부에서 이루어지는 통신에 접근할 수 있게 된다. 두 번째 예외조항은 '근로자의 동의'에 따른 예외인데, 회사는 근로자의 동의하에 인터넷과 이메일을 감시할 수 있게 된다. 근로자가 동의를 거부하는 경우 좋지 않은 결과가 있을 것이며 묵시적인 동의로도 충분하기 때문에 이러한 동의는 손쉽게 확보할 수 있다. 특히 사용자가 직원들을 감시함에 있어 이메일에 대한 감시사실을 사전 고지할 것이므로, 이때 묵시적인 동의가 있는 것으로 간주될 것이다.[36] 세 번째 예외는 '일상 고용관계'에 따른 예외이다. 만일 회사 자산의 보호를 위하여 감시가 필요했다거나 통신서비스의 원활한 제공을 위하여 감시가 행하여졌다는 사실을 사용자가 입증할 수 있다면 본 예외조항이 적용되게 된다.[37] 이러한 예외조항 중 하나가 적용된다면, ECPA법은 감시 방식이나 그 정도를 제한하지 않으며, 사용자가 근로자에게 감시사실을 고지할 필요도 없게 된다.[38] 그러나 이 중 '일상 고용관계'에 따른 예외의 경우 판례법은 사용자가 근로자에게 감시사실을 고지할 의무를 부과하고 있다.[39]

상기 설명과 관련하여 이메일이나 컴퓨터 폴더 상에 '사적인 정보'임을 별도로 표시한다 할지라도 이러한 이메일이나 폴더를 사용자가 감시할 수 있는 권리는 영향을 받지 않는다는 사실이 중요하다.[40] 종이 우편이나 개인 사물함과

35) *18 USCS 2510 (2007).*
36) Rustad & Paulsson, supra note 2, at 29.
37) *Arias v. Mut. Ctr. Alarm Serv., 182 F.R.D. 407* (S.D.N.Y. Sept. 11, 1998); see also Rustad & Paulsson, supra note 2, at 32.
38) Kesan, supra note 8, at 299.
39) *Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001)*; Rustad & Paulsson, supra note 2, at 30.
40) *Vernars v. Young, 539 F.2d 966 (3rd Cir. 1976).*

관련된 초기 판결들은 사적인 우편물이나 사물함 속의 개인 소유물에 대해 각 개인이 프라이버시에 대한 정당한 기대를 가질 수 있다고 보았다.[41] 'Vernars' 사례에서 법원은 사적인 우편물이라고 표시되어 각 개인 앞으로 송부된 사적 편지의 경우 회사 사무실로 배달이 되었다 할지라도 권한 없는 자가 이를 개봉할 수도 읽을 수도 없다고 판시하였다.[42] 현재까지 어떠한 법원도 이러한 판례를 사적인 이메일과 업무용 이메일을 구별하기 위해 적용한 바 없다.[43] 이러한 차이점을 뒷받침하기 위해 지지하는 주장은 개인사물함과 컴퓨터의 차이점에 있어서는 개인 사물함의 경우 개인 소유물을 보관하기 위한 목적으로 사용자가 제공한 것이나 컴퓨터의 경우 순전히 업무목적을 위해서만 제공된다고 설명한다.[44] 또한, 네트워크상에서 전송 중인 이메일의 경우 그 접근 가능성이 있으므로 밀봉된 편지와 이메일에 있어 프라이버시에 대한 정당한 기대가 다를 수 밖에 없다고 한다. 이러한 주장을 통해 심지어 비밀번호를 설정하여 저장한 이메일에 대한 보호 또한 배제되어야 한다고 한다.[45]

다. 노동법

사용자에 의한 인터넷이나 이메일 감시로부터 근로자를 보호하는 데 있어 미국에서는 노동법의 역할은 그다지 크지 않다.[46] 개별적인 고용계약과 일반적인 행동규범(codes of conduct)의 범위 내에서 사용자는 사업장 내에서의 인터넷과 이메일의 사용과 통제에 대해 자유롭게 결정할 수 있다.[47] 고용계약이나 행동규범들이 구체적인 법률 규정에 의해 제한을 받지 않으므로 근로자의 입장에서는 이를 수용할 수 밖에 없게 된다.[48] 물론 근로자들이 단체교섭을 통해 사용

41) Id.; *K-Mart v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984).*
42) *Vernars, 539 F.2d 966.*
43) Rustad & Paulsson, supra note 2, at 25.
44) *McLaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 (Ct. App. 1999).*
45) Rustad & Paulsson, supra note 2, at 40.
46) Matthew T. Bodie, The Potential for State Labor Law: The New York Greengrocer Code of Conduct, *21 Hofstra Lab. & Emp. L.J. 183, 185 (2003).* See *11 U.S.C. 365 (2006).*
47) Blanpain & Colucci, supra note 5, at 138.
48) 이러한 관행은 프라이버시의 관점에서도 비판받고 있다. See, e.g., Phillips, supra note 22, at 59.

자가 감시시스템으로부터 취득한 정보를 사용하는 데 일정 정도 제한을 가할 수는 있다. 그렇지만 이러한 보호는 노동조합에 가입한 근로자에게만 가능한 것이기도 하다.[49]

고용관계의 해지에 있어서는 임의고용의 원칙(doctrine of employment at-will)이 일반적으로 적용된다.[50] 본 원칙에 따를 경우 사용자는 근로자와 언제든 이유 없이 고용관계를 해지할 수 있는 무제한의 재량을 갖는다. 심지어 잘못된 정보를 바탕으로 고용관계를 해지하였고 이로 인하여 법적인 측면에서 책임이 인정된다 할지라도 이러한 재량권은 인정된다.[51] 근로자가 사용자에 비해 약자의 위치에 있다는 인식이 높아짐에 따라 판례법에서 임의고용의 원칙에 대해 몇몇 예외들이 인정되어 왔고 이와 함께 동 원칙의 효력이 지난 몇 년간 약화되었다.[52] 이러한 예외의 인정은 각 주 별로 차이가 있다.[53] 가장 일반적으로 인정되는 세 가지 예외로는 (ⅰ) 고용관계의 지속에 관하여 묵시적으로 인정된 계약상 권리 위반,[54] (ⅱ) 공공질서에 반한 고용관계의 해지, (ⅲ) 신의성실과 공정한 거래에 대한 묵시적 합의의 위반이 있다.[55] 이러한 예외는 주로 고용관계의 해지에 관한 계약상 또는 묵시적 절차의 존재 및 그 위반과 고용관계의

49) Yung, supra note 35, at 181.

50) Jacobs, supra note 5.

51) See Electronic Privacy Information Center, Workplace Privacy, http://www.epic.org/privacy/workplace.

52) See, e.g., Title VII of the Civil Rights Act of 1964, *42 U.S.C. 2000* (2007); Civil Rights Act of 1991, *42 U.S.C. 2000* (2000); National Labor Relations Act, *29 U.S.C. 158* (1968); Age Discrimination in Employment Act of 1967, *29 U.S.C. 621* (2001); Americans with Disabilities Act of 1992, 42 U.S.C 12101 (2000); see also David H. Autor, Outsourcing at Will: The Contribution of Unjust Dismissal Doctrine to the Growth of Employment Outsourcing, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=281418; Engeline Grace van Arkel, A Just Cause for Dismissal in the United States and the Netherlands (Doctoral Thesis, Erasmus University Rotterdam), http://publishing.eur.nl/ir/repub/asset/9080/001-552_536974.pdf

53) See, e.g., *Smyth vs. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).*

54) Jacobs, supra note 5, at 214.

55) 모든 주들이 세 가지 예외를 인정하는 것은 아니다. See generally Charles Muhl, The employment-at-Will Doctrine: Three Major Exceptions, Monthly Labor Review, Jan. 4 2001.

해지에 관한 정당한 이유의 부재에 초점을 맞추고 있다.[56] 인터넷이나 이메일 감시를 통하여 수집한 정보를 바탕으로 한 해고에 관한 사례에 있어, 정당한 사유(just cause) 자체는 문제가 되지 않는다. 이러한 정당한 사유를 취득하는 방식이 정당한지 여부와 증거의 채택가능성 여부가 다투어진다. 인터넷이나 이메일 감시에 있어 근로자가 주장할 수 있는 가장 좋은 법적 근거는 프라이버시권이 침해되었으므로 공공질서에 반한 부적법한 고용해지임을 주장하는 것이다.[57] 'Borse' 사례에서 항소법원은 근로자의 해고가 사생활의 침해와 관련된 경우에 있어 다음과 같은 예측을 한 바 있다. 펜실베니아 대법원은 문제가 되고 있는 사생활 침해와 관련된 사실과 배경을 조사할 것이다.[58] 만일 해고가 상당하면서 아주 심할 정도로 직원의 사생활을 침해하였다고 법원이 판단한다면 이러한 해고는 공공질서에 반한다는 결론을 내리게 될 것이다.[59] 'Smyth' 사례에서 임의고용의 원칙에 대하여 공공질서에 근거한 예외가 인정되기 위해서는 공공질서에 관한 명확한 근거가 있어야 한다고 법원은 보았으며, 이러한 명확한 근거는 '사생활의 침해'에 대하여 당해 주(state)의 보통법상 불법행위책임으로 구체화되어 있어야 한다고 보았다. 따라서 불법적인 고용 해지에 대한 구제책을 노동법에서 찾는다 할지라도 다시 프라이버시법(privacy law)에 대한 검토는 필요하게 된다. 위에서 설명한 바와 같이 사생활에 대한 침해가 인정되기 위해서는 프라이버시에 대한 정당한 기대가 인정되어야 한다. 이메일과 인터넷에 있어서는 이러한 정당한 기대가 인정되기는 힘들다. 또 다른 측면에서의 문제점은 근로자를 감시할 수 있는 권한이 증가함에 따라 근로자의 인터넷 접속과 관련하여 잘못된 판단을 할 수도 있다는 것이다.[60] 전자개인정보센터(the Electronic Privacy Information Center: EPIC)의 웹사이트상에는 다음과

56) 정당한 사유 요건은 부당해고에 관한 주법에서만 중요성을 갖는다. 예를 들어 Montana Wrongful Discharge from Employment Act, *Mont. Code ANN. 39-2-901* (1987).

57) Jacobs, supra note 5, at 226.

58) *Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3rd Cir. 1992).*

59) Id.

60) See Office of the Federal Privacy Commissioner, Speaking notes for Malcolm Crompton, Federal Privacy Commissioner, Current Workplace Privacy Issues (Oct. 23, 2003), available at http://www.privacy.gov.au/materials/types/speeches/ view/6401

같은 사례가 제시되어 있다: 근로자가 'whitehouse.gov'에 접속하려다가 실수로 포르노 사이트인 'whitehouse.com'에 접속할 수도 있다. 이 때 네트워크 감시장비는 근로자의 의도를 감안하지 않고 부적절한 사이트 접속으로 이를 감지할 수 있을 것이다.[61] 이처럼 근로자에 대하여 잘못된 판단을 내릴 수 있는 가능성으로 인해 고지를 받을 권리나 발언권 등 적절한 보호 절차를 갖출 필요성은 증가하게 된다.

라. 정보 보호

두 개의 법령을 통해 정보보호에 대한 규제를 하고 있는 유럽과 달리 미국에는 정보보호를 위한 연방법률이 존재하지 않는다.[62] 따라서, 미국에 있어서는 (ⅰ) 감시 객체에게 접근권이나 정보수정권이 있는 경우, (ⅱ) 정보의 사용이나 공개를 제한할 수 있는 구체적인 목적이 요구되는 경우, (ⅲ) 정보처리방침이나, (ⅳ) 여타 기본적인 공정 정보사용 관행이 있는 경우[63]가 아니라면 정보보호를 기대하기 힘들다. 또한 미국에는 분쟁을 해결할 권한을 가지거나 사생활 침해 주체에게 벌금을 부과하거나 기타 행정명령을 내릴 수 있는 정보보호 관련 정부기관이 존재하지 않는다. 법원에서의 분쟁 해결이 실질적인 해결책이 되지 못하기 때문에 이러한 정부기관의 부재는 문제가 될 수 있다. 일단 소송은 비용이 많이 들며, 원고의 입장에서는 소송을 수행할만한 변호인을 찾기가 쉽지 않으며, 실제로 구제를 받을 가능성 또한 불확실하기 때문이다.[64] 또한, 부당해고의 경우 변호사를 찾는 데 문제가 있는데, 이는 민사 변호사들의 경우 손해배상에 따라 높은 수임료가 예상될 때에만 소송을 맡으려 하기 때문이다.[65] 위

61) See Electronic Information Privacy Center, Workpalce Privacy, http://www.epic.org/privacy/workplace/

62) European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 of 31 July 2002.

63) See Gellman, supra note 14.

64) Id.

에서 언급한대로 불법적인 인터넷과 이메일 감시를 근거로 한 부당해고소송에서 승소할 가능성은 무척 제한적이다. 하지만 부당해고로 판정이 된다면 미국법하에서의 배상액이 네덜란드에서의 경우보다 상당히 높기는 하다.[66]

마. 근로자의 행위에 대한 사용자의 책임

사용자책임에 있어 엄격책임주의(strict liability doctrine of respondeat superior)가 폭넓게 인정되는 최근 경향에 따라 사용자는 근로자의 예상 가능한 불법행위책임이나 범죄에 대하여 엄격책임을 부담하여야 한다.[67] 사용자에게 있어 성희롱 케이스로 인한 리스크가 있을 수 있다. 성희롱 관련 대책 및 이러한 대책에 대한 시행이 없다면 직장 내 성희롱 사건으로 인해 사용자는 책임을 부담할 리스크를 지게 된다.[68] 이외에도 직원들의 인터넷이나 이메일 사용으로 인해 사용자의 책임이 될 수 있는 불법적인 행위가 생겨날 수 있는 리스크가 있게 된다.[69] 근로자의 행동으로 인해 책임을 지게 될 부담이 늘어남에 따라 이들을 긴밀히 감시할 이유 또한 생겨나게 된다고 많은 문헌들이 언급하고 있다.[70] 근로자의 근무시간 이외의 활동이라 할지라도 예를 들어 사용자책임이 문제될 수 있는 협박이나 사업장 내 안전과 관련이 있는 경우라면 사용자가 근로자의 활동을 감시할 정당한 근거가 된다.[71] 따라서 일정한 경우 근로자의 사

65) Jacobs, supra note 5, at 227.
66) Id. At 219.
67) Kesan, supra note 8, at 311 (referring to M. Ishman, 'Comment', Computer Crimes and the Respondeat Superior Doctrine: Employers Beware, *6 B.U. J. Sci. & Tech. L. 6 (2000)* and J.E. Davidson, Reconciling the Tension Between Employer Liability and Employee Privacy, *8 Geo. Mason U. Civ. Rts. L.J. 145, 147 (1997)*.
68) See B.P. Miller, Title VII Affirmative Defense in the Real World: Recent Application of Ellerth / Faragher and What They Require, available at http://papers.ssrn.com/sol3/papers.cfm?abstract id=909661 (Aug. 28, 2005).
69) See Proofpoint Inc., Outbound Email and Content Security in Today's Enterprise, 2009, http://www.proofpoint.com/id/outbound/index.php?
70) See Phillips, note 31; see also Amanda Richman, Restoring the Balance: Employer Liability and Employee Privacy, (2000～2001); Contra Yung, supra note 35, at 222.
71) Jonathan Canter, Drawing the Line on Privacy at Work, http://www.careerjournal.com

생활이 사업장에서의 책임에 영향을 미치느냐에 따라 근로자의 사생활에 대해서도 사용자가 정당한 이해관계를 가지게 된다. 사용자가 책임을 부담할 리스크는 일반적인 고용 관계에서뿐만 아니라, 공동사용자관계에서도 발생하게 된다.[72] 공동사용자(Co-employment)란 두 개의 업체가 동시에 한 직원의 업무나 업무 환경에 대하여 영향을 미치게 되는 경우 적용되는 법 원리를 말한다.[73] 임시 근로자를 공급하는 업체와 이러한 업체로부터 근로자를 공급받는 업체간의 관계가 전형적인 예이다.[74] 2003년 이래로 아웃소싱(outsourcing)은 공동사용자관계로 간주되었다.[75] 이와 관련하여 고용관계 내에서의 사생활 보호를 향상시키기 위하여 근로자의 부정행위(fraudulent behavior)에 대한 사용자의 책임을 완화할 필요가 있게 된다.

바. 결론

사업장내에서의 사생활에 관한 구체적인 권리는 물론, 프라이버시권 일반에 관한 법률이 미국 내에는 존재하지 않는다. 사용자에 의해 인터넷과 이메일 감시가 있는 경우 근로자는 (ⅰ) 제4차 연방수정헌법, (ⅱ) 사생활의 침해에 따른 불법행위책임, (ⅲ) ECPA법이라는 세 가지 법원을 활용할 수 있다. 이중 제4차 연방수정헌법과 사생활의 침해에 따른 불법행위책임의 경우 프라이버시에 대한 정당한 기대라는 요건으로 인해 사생활에 대한 적절한 보호를 기대하기 힘들다. 우선 사용자가 감시(또는 감시의 가능성)에 대해 고지를 한 경우 근로자는 프라이버시에 대한 정당한 기대를 더 이상 가질 수 없게 된다. 다음으로, 사용자가 제공하는 각종 자산을 활용하는 경우 근로자는 프라이버시권을 포기한 것으로 간주된다. 심지어 프라이버시에 대한 정당한 기대가 인정된 경우라 할지라도 사내 이메일 시스템에서 이루어지는 부적절하거나 직업윤리에 어긋나는 통신을 방지할 사용자의 정당한 이익이 근로자의 정당한 기대보다 우선하게 된다. ECPA법의 경우 본 법상 인정되는 예외조항들로 인해 고용관계에서의 사생활

/myc/legal/19990209-canter.html; Yung, supra note 35, at 193.

72) Ronald E. Wainrib, Co-employment Raises New Legal Risks in Contingent Workforce Management, Jan. 15, 2005, http://www.contingentlaw.com/ Coemployment.htm

73) See id.

74) Id.

75) Id. Zheng v. Liberty Apparel Co. Inc, No. 02-7826 (2d Cir. Dec. 30, 2003).

보호가 사실상 인정되기 힘들다. 이는 사용자가 제공하는 컴퓨터 네트워크를 근로자가 사용하는 경우 사용자가 이를 감시하는 데 묵시적으로 동의한 것으로 간주되기 때문이다. 사용자가 예외조항 중 하나의 요건을 충족하는 경우 ECPA 법은 감시 방법이나 정도를 제한하지 않으며, 심지어는 감시에 대해 사용자가 근로자에게 고지할 의무도 요구하지 않게 된다.

개별적인 고용계약이나 일반적인 행동규범(codes of conduct)의 범위 내에서 사용자는 사내에서 이루어지는 인터넷과 이메일통신의 이용과 통제를 자유롭게 결정할 수 있다. 이러한 계약이나 행동규범이 관련 법령에 의한 제한을 받지 않으므로, 근로자는 어쩔 수 없이 이를 수용할 수 밖에 없다. 사업장내에서 근로자의 사생활에 대한 권리를 향상시키기 위해서 이메일과 인터넷 감시를 시행하기 전에 분명하고 명확한 고지를 할 것이 강조되고 있다. 그러나 사용자의 감시권에 대한 금지나 제한에 대해서는 크게 언급되지 않고 있다.[76] 몇몇 주에서 이러한 금지나 제한에 대한 입법안이 제출되었으나 실제로 법제화된 바는 없다. 따라서 인터넷과 이메일 감시에 있어 근로자에 대한 더 큰 법적 보호를 미국에서 이른 시일 내에 기대할 수는 없는 실정이다.[77] 프라이버시법과 마찬가지로 노동법 또한 직원들의 사생활을 침해하는 사용자의 행위로부터 근로자들을 보호하지는 못한다. 우선 이는 임의고용의 원칙이 여전히 일반적으로 적용되고 있기 때문이다. 다음으로 인터넷과 이메일 감시를 근거로 한 부당해고의 경우 이에 대한 예외의 문제, 즉, 근로자가 프라이버시에 대한 정당한 기대를 가졌는지가 다시 문제가 되기 때문이다.

사용자에 의한 프라이버시 침해가 있었음을 주장하기 힘든 다른 이유는 소송 자체가 실질적인 해결책이 되지 못하기 때문이다. 그 이유는 (ⅰ) 소송비용이 많이 들며, (ⅱ) 이러한 소송을 수행할 변호사를 구하기 힘들며, (ⅲ) 손해액을 입증하기 곤란하고, (ⅳ) 승소 가능성이 불분명하기 때문이다. 이런 측면에서 볼 때, 미국 내에서 정보보호기관의 부재와 공정한 정보처리관행에 대한 고려가 거의 존재하지 않는다는 사실은 사업장 내에서 근로자들의 사생활이 보호받는 것을 더욱 어렵게 한다. 마지막으로 사용자책임과 관련된 법령으로 인해 사용

76) 예컨대, Privacy for Consumers and Workers Act (1993, Senator Paul Simon), Notice of Electronic Monitoring Act (2000, Senator Charles Schumer).

77) See id.

자는 근로자의 행동을 폭넓게 감시할 정당한 이유를 갖게 된다.

위에서 검토한 바에 따를 경우 미국의 근로자들은 사업장내 인터넷과 이메일 사용에 있어 프라이버시권을 전혀 인정받지 못하고 있다는 일반적인 결론에 이르게 된다.

3. 네덜란드의 접근방식

가. 개요

여기서는 네덜란드 사업장에서의 인터넷과 이메일의 사용과 통제를 규제하는 각종 법률을 다루고자 한다. 네덜란드에는 사업장 내 프라이버시에 대해 규율하는 별도의 법률이 존재하지 않는다. 노동법과 프라이버시법에 규정된 일반적인 법령에 의하여 판결이 내려진다. 판례법에 따를 경우 네덜란드에서는 유사한 사안들임에도 불구하고 각기 다른 법률적 근거에 의해 다루어진 바 있다. 이러한 법률적 근거와 무관하게 이러한 사안들에 있어 그 결과는 차이가 났다. 따라서 네덜란드에서 사업장 내 인터넷과 이메일 감시에 관한 일반적 결론을 내는 일은 쉽지 않다. 그럼에도 불구하고 일반적인 특징을 찾을 수 있으며 이는 미국에서의 인터넷과 이메일 감시와 비교하여 흥미로운 대조를 이룬다.

나. 인권

네덜란드에서 프라이버시권에 대한 접근방식은 '인권과 기본적 자유의 보호를 위한 유럽협약(the European Convention for the Protection of Human Rights and Fundamental Freedoms, 이하 유럽인권협약)'에 근간을 두고 있다.[78] 네덜란드 헌법 제10조는 유럽인권협약의 관련 조항과 일치한다.[79] 미국

78) Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005, Rome 4 November 1950; European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector(Directive on privacy and electronic communications),

과는 대조적으로 네덜란드 헌법을 포함한 유럽의 법령들은 개인 정보의 처리에 있어 사생활의 보호에 대한 권리를 명시적으로 인정한다.[80] Westin은 이러한 관념을 정보에 대한 프라이버시(informational privacy)라고 이름 붙였으며, 이 개념은 유럽에서 널리 알려지게 되었다.[81] 사업장 내에서의 프라이버시권에 대해 회의적인 미국과 달리 유럽인권법원(the European Court of Human Rights)은 유럽인권협약 제8조를 기초로 하여 이를 명시적으로 인정하였다.[82] 본 제8조와 네덜란드 헌법 제10조는 공공 사용자(public employers)는 물론 민간 사용자(private employers)에게도 적용될 수 있다.[83][84] 사업장 내에서 프라이버시권이 명시적으로 인정됨에도 불구하고 네덜란드 판례법에 따를 경우 사용자에 의한 인터넷과 이메일 감시에 있어 이러한 프라이버시권이 인용되는 경우는 흔치 않다.[85] 대신 노동법상 개념들과 같은 다른 법적 근거들이 근로자의

Official Journal L 201 of 31 July 2002.

79) Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815, Stb. 1987, 458.

80) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002. Official Journal L 201, 31/07/2002 P. 0037-0047; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31-50 and article 10 of the Dutch Constitution.

81) Alan F. Westin, Privacy and Freedom (The Boldley Head) (1967).

82) [역주] 유럽인권협약 제8조(사생활 및 가족생활을 존중받을 권리)
1. 모든 사람은 그의 사생활, 가정생활, 주거 및 통신을 존중받을 권리를 가진다.
2. 법률에 합치되고, 국가안보, 공공의 안전 또는 국가의 경제적 복리, 질서유지와 범죄의 방지, 보건 및 도덕의 보호, 또는 다른 사람의 권리 및 자유를 보호하기 위하여 민주사회에서 필요한 경우 이외에는, 이 권리의 행사에 대하여는 어떠한 공공당국의 개입도 있어서는 아니된다.; Eur. Ct. H. R. 16 December 1992 (Niemietz) and Eur. Ct. H. R. 25 June 1997 (Halford).

83) Dutch Supreme Court, 19 January 1987, Nederlandse Jurisprudentie (NJ, Dutch Case Law) 1987/928.

84) Dutch Const. art. 10. Translation from Hendrickx, F., Privacy and Data Protection in the Workplace: The Netherlands, in: Siaak Nouwt, C. Prins, & Berend Vries, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy 140, Information Technology & Law Series 7 (The Hague: T.M.C. Asser Press) (2005).

프라이버시 침해에 있어 사용자에 대해 소를 제기하기 위해 인용된다.

다. 노동법

미국에서와 마찬가지로 네덜란드에서도 근로자가 인터넷과 이메일을 사용함으로써 리스크가 발생하기 때문에 사용자가 이를 감시하는 것은 정당화된다. 네덜란드 민법 제7:660조(Article 7:660 of the Dutch Civil Code)는 고용관계 내에서 사용자가 근로자에 대해 일정한 권한을 가질 수 있음을 규정하고 있다. 네덜란드 민법 제7:661조와 제6:162조는 이러한 권한을 제한한다. 사용자는 성실한 사용자(good employer)이어야 하며, 그의 행동 또한 적법하여야 한다.[86] 네덜란드에서 인터넷과 이메일 감시의 적법성 여부는 주로 부당해고 관련 소송에서 다루어진다.[87] 그렇지만 감시 자체의 적법성이 다투어지는 것은 아니다. 소송의 쟁점이 되는 것은 감시를 통해서 수집한 증거를 바탕으로 한 근로자를 해고한 것이 적법한지 여부이다. 고용관계의 해지와 이와 관련된 사용자에 의한 인터넷과 이메일 감시의 적법성 여부는 당해 소송과 관련된 사실관계의 평가에 의해 결정된다. 법적 근거에 대한 고려 없이 사용자와 근로자의 이익간 균형에 초점이 맞추어지곤 한다. 아래에서 설명하는 바와 같이 노동법 내에서 프라이버시에 대한 기본권과 정보보호권이 적절하게 이용되지 않는데 대해 네덜란드의 프라이버시 보호주의자들은 신랄하게 비판하고 있다.[88] 소송은 유럽

85) Homan, infra note 88; see, Blanpain, supra note 8, at 95-124; see also Hendrickx, supra note 86.

86) 미국에서도 계약법상 유사한 의무가 존재한다("the duty of good faith and fair dealing"). 이 의무는 근로계약에도 적용되지만 실질적인 의미는 제한적이다. 네덜란드 민법 7:611조는 사용자에게 성실한 사용자의 의무를 요구할 뿐만 아니라, 근로자에게도 성실한 근로자의 의무를 요구하고 있다.

87) 이것은 네덜란드가 부당해고에 대해서는 매우 엄격한 제도를 갖고 있는 반면 프라이버시 위반에 대해서는 보상의 거의 인정하고 있지 않다는 사실을 통해 설명된다. See Cuijpers, C.M.K.C., De prijs van privacy, Computer & R 6:272 '04.

88) Hendrickx, supra note 86, at 141; M.A.C. de Wit, Het goed werkgeverschap als intermediair van normen in het arbeidsrecht 161-164, Deventer: Kluwer (1999); D.J. Kolk and M. Verbruggen, Het verborgen bestaan van de Wet bescherming persoonsgegevens 3-10, Arbeids R. 6/7 '02.; L. Bijlsma and T.C.B. Homan, Toepassing Wbp door Kantonrechter bij ontslag werknemer, de Wbp ontslagen? 167 (No. 5 Arbeid Integraal 2003).

인권협약 제8조나 네덜란드 헌법 제10조를 직접적인 근거로 제기되기도 하지만 프라이버시권은 네덜란드 민법 제7:661조와 제6:162조의 해석에 의해 도출될 수도 있다. 그렇지만 판사들이 프라이버시 및 정보 보호와 관련된 쟁점을 심각하게 고려하는 것으로 보이지는 않는다. 이는 사용자에 의한 인터넷과 이메일 감시 관련 사례에 있어 네덜란드 법정에서는 프라이버시와 정보보호에 대한 소가 제기되지 않는 주된 원인이 된다. 이러한 소송에 있어 주로 고려되는 세 가지 요소는 (ⅰ) 선택된 통제 방식에 대한 충분한 법적 근거가 있는지 여부, (ⅱ) 비례의 원칙과 보충성의 원칙,[89] (ⅲ) 인터넷과 이메일 사용 방침에 대한 회사 규정이 있는지 여부이다. 사용자가 인터넷과 이메일 감시 기술을 부당하게 활용하여 부당해고가 된 사안들에 있어 근로자의 인터넷과 이메일 사용에 관한 방침이 있는지 여부가 결정적이었음을 판례법은 보여주고 있다.[90] 일반적으로 적절한 행동규범(code of conduct)이 갖춰진 경우에는 해고가 정당화되는 반면 그렇지 않은 경우 해고가 무효로 될 수 있다. 회사의 행동규범의 존재에 대해서 근로자에게 적절한 고지가 이루어져야 한다. 이와 함께 행동규범은 (ⅰ) 근로자의 인터넷과 이메일 사용, (ⅱ) 이러한 사용이 사용자에 의해 통제되는 방식, (ⅲ) 행동규범을 위반하여 사용한 경우 책임에 대한 규정을 담고 있어야 한다.

네덜란드는 부당해고에 있어 근로자를 보호하기 위한 엄격한 법령을 갖추고 있다. 그렇지만 근로자의 부정행위(fraudulent behavior)는 대부분의 사례에 있어 해고를 정당화한다.[91] 근로자의 부정행위에 대한 증거를 수집함에 있어 근로자의 프라이버시권을 침해했다 할지라도 이것이 해고의 적법성 여부에 대한

89) 비례의 원칙과 보충성의 원칙에 따라 인터넷과 이메일에 대한 감시는 의도한 목적을 달성하는데 필요한 범위를 넘어서는 안 되며, 가능하다면 침해의 정도가 덜한 수단에 의해야 한다.

90) J. Bom, Rechters toetsen gedragscodes 16-18; People Planit Profit(Autumn 2003), http://www.p-plus.nl/beelden/rechters.pdf. 최근 판례에 의하면 영상감시는 사용자가 근로자에게 통지한 경우에만 허용될 수 있다. 사용자는 근로자에게 이러한 영상감시의 가능 사용 범위에 대해 적절히 통지하여야 하며 이를 게을리한 경우, 감시에 의해 수집된 증거에 기해 행해진 해고는 무효가 된다. Aarticles 139f and 441b. LJN: AR8052, Rechtbank Haarlem, 22-12-2004, 108067 / KG ZA 04-630, available at www.rechtspraak.nl).

91) See Hendrickx, supra note 86, at 141; Kolk and Verbruggen, supra note 90; Bijlsma and Homan, supra note 90.

법원의 결정에 대부분 영향을 미치지 않는다. 현재의 판례법에 따르면 원고의 프라이버시권에 대한 침해로 인하여 법적 책임이 발생하는 경우는 흔치 않다. 프라이버시권이 침해되었다는 결정이 있었다 할지라도 종종 이러한 침해는 정당하다는 판결이 나게 된다.[92] 이러한 침해가 정당하지 않다 할지라도 판례법에 따를 경우 근로자가 반드시 복직되는 것은 아니며, 증거가 효력을 반드시 잃는 것도 아니며, 사용자가 손해배상을 해야 할 의무가 반드시 발생하는 것도 아니다.[93] 심지어는 유럽의 판례법에 따를 경우, 용의자의 프라이버시권을 침해하면서 수집된 증거라 할지라도 형사소송에 있어 반드시 그 증거력을 상실하는 것은 아니다.[94] 이러한 판결의 내용이 근로자의 프라이버시권을 침해하여 수집한 근로자의 부정행위에 대한 증거에 대해서도 적용될 수 있을 것으로 보인다.[95] 개인적인 생각으로는 프라이버시권의 침해에 대한 구제책의 부재는 네덜란드의 프라이버시 보호에 있어 큰 흠결로 여겨진다.

라. 개인정보보호법

개인정보보호법(Personal Data Protection Act: PDPA)은 개인정보의 처리를 규제하는 구체적인 규정들을 담고 있다.[96] 인터넷과 이메일 사용을 감시하는 사용자는 개인정보를 처리하게 되며, 따라서 결국 개인정보보호법의 규제를 받게 된다. 위에서 언급된 바와 같이 네덜란드 법원에 제기되는 사업장장 내 프라이버시 관련 소송에 있어 개인정보보호법이 문제되는 경우는 거의 없다.[97]

---

92) Dutch Supreme Court, 27 April 2001, NJ 2001/421 (Wennekes).

93) Id.; See P. de Hert and B-J Koops, Privacy is nog steeds een grondrecht. Pleidooi voor de uitsluiting van onrechtmatig bewijs', Ars Aequi 50 972-975 (2001); Dutch Supreme Court, 27 April 2001, NJ 2002/91.

94) See Kahn v. United Kingdom, 2000 ECHR (2007).

95) De Hert and Koops, supra note 94.

96) 동법은 개인정보의 처리 및 자유로운 이동과 관련 개인의 권리 보호에 관한 Directive 95/46/EC의 이행을 위하여 제정되었다. Official Journal L 281 of 23.11.1995. Directive 95/46/EC에 규정된 것처럼 개인정보의 처리에 관한 규정은 사업장 내 감시시스템의 이용에 관해서도 적용될 수 있다(Article 29 Data Protection Working Group, Opinion 8/2001).

97) Hendrickx, supra note 86, at 141 (referring to de Wit, supra note 86, at 161-164 and Kolk and Verbruggen, supra note 90, at 3-10).

고용관계에 있어 정보보호가 거의 존재하지 않게 된 이유는 판사들이 동일한 결론을 '성실한 사용자의 원칙(good employership)'을 통해서도 도출할 수 있다고 믿기 때문일 것이다.[98] 그렇지만 이는 개인정보보호법이 '성실한 사용자의 원칙'이 가지고 있는 애매모호함에 명확성을 가져다 줄 수 있다는 점을 간과한 것이다. '성실한 사용자의 원칙'을 바탕으로 하여 양자의 이익을 조정하는 데 있어 개인정보보호법은 참고가 될 수 있다. 더욱이 개인정보보호법은 권리와 의무를 명확하게 규정하고 있으며, 인터넷과 이메일 감시의 적법성 여부에 대한 분명한 답을 얻기 위하여 개인정보보호법상 권리와 의무의 위반 여부가 평가되어야 한다. 개인정보보호법의 핵심 규정은 일반 조항 형태로 규정되어 있는데, 이는 개인정보의 처리가 공정하고 적법할 것을 요구하고 있다. 정보처리가 이러한 기준을 충족하기 위해 준수되어야 할 권리와 의무가 개인정보보호법상에 규정되어 있다.[99]

간단히 말하면 개인정보보호법은 개인정보의 처리가 정당한 목적을 가지고 있을 것을 요구하며 처리 수단 또한 목적에 비추어 적절해야 할 것을 요구하고 있다. 또한 목적과 맞지 않는 방식으로 수집한 정보를 처리할 수 없도록 하고 있다. 더 나아가 개인정보보호법은 개인정보의 처리가 이루어질 수 있는 법적 요건들을 상세히 규정하고 있다.[100] 미국과 비교하여 이러한 요건 중 하나가 근로자의 동의라는 점이 중요하다. 미국에서는 근로자의 동의를 손쉽게 확보할 수 있다. 그러나 동의가 근로자의 자유의사에 의해 주어져야 한다는 네덜란드 법의 요건으로 인해 고용관계에서는 동의 자체가 효력이 없다고 해석될 수도 있다.[101] 이는 근로자가 사용자에 비해 열위의 입장에 있기 때문이다. 따라서 인터넷과 이메일 감시는 다른 요건도 충족하여야 하며 이는 주로 사용자의 정당한 이익이 된다. 이는 '프라이버시 점검(privacy check)'을 수반하게 되며 즉 근로자를 감시할 사용자의 이익이 프라이버시에 대한 근로자의 이익보다 큰 경우에만 감시가 이루어질 수 있다는 것이다. 감시의 목적 및 요건과 관련된 규

98) Hendrickx, supra note 86, at 141.
99) Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Stb. 2000, 302.
100) Id. Article 8.
101) Opinion 8/2001 of the Article 29 Working Party (2001), available at http://ec.europa.eu/justice_ home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

제사항 이외에도 개인정보보호법은 정보, 보안, 기밀성과 관련한 사용자의 의무는 물론 근로자가 본인의 개인정보에 접근하고 수정할 권리를 규정하고 있으며, 이러한 정보의 수집을 거부할 권리 또한 포함하고 있다.[102]

개인정보보호법과 관련하여 마지막으로 설명될 사항은 국가정보보호국(National Data Protection Authority: NDPA)에 대해서이다.[103] 국가정보보호국은 개인정보보호법의 시행 여부를 감시할 책임을 지고 있다. 국가정보보호국은 자문역할을 수행하며 개인정보보호법과 관련된 분쟁을 해결한다. 또한 본 기관은 조사권이 있으며 벌금을 부과할 권한을 가지고 있다. 국가정보보호국은 근로자의 인터넷과 이메일 사용 감시에 대하여 사용자가 적절한 방침을 갖추는 데 도움이 될 기본규칙을 발간한 바 있다.[104] 네덜란드 법원이 판결을 내리는 데 있어 이러한 기본규칙은 참고가 될 수 있다. 그렇지만 인터넷과 이메일 감시에 대한 네덜란드 판례법에 있어 이러한 기본규칙이 언급된 바가 없다는 사실은 그리 놀랄 일은 아니다. 왜냐하면 인터넷과 이메일 감시 관련 소송에서 프라이버시권과 정보보호권은 대개 고려되지 않기 때문이다.

마. 근로자의 행동에 대한 사용자의 책임

네덜란드 민법은 근로자의 행동에 대한 사용자책임과 관련된 규정을 두고 있다.[105] 그러나 이러한 책임은 '업무 활동 범위 내의 부정한 행위(tortuous acts within the scope of his working activities)'에 대한 것으로 제한되어 있다.[106] 근무시간 이내라도 사용자의 자산에 대한 사적 이용이 이러한 범위에 포함되는 것으로 해석될 수 있을 지는 의문스럽다. 필자가 아는 범위에서 근로자가 사용자의 인터넷이나 이메일을 사용했다고 하여 근로자가 행한 부정한 행위에 대하여 사용자가 책임을 져야 한다고 하는 네덜란드 법원의 판례는 없다. 사용자가 책임을 져야 한다면 사용자는 이를 근로자의 고의적이거나 부주의한 행위를 이유로 하여 근로자로부터 구상 받을 수 있을 것이다. 그렇다고 하더라도 사용자

102) Hendrickx, supra note 86, at ch. 2 and 6.
103) College Bescherming Persoonsgegevens, CBP News, http://www.cbpweb.nl
104) College Bescherming Persoonsgegevens, Goed werken in netwerken, April 2002, available at www.cbpweb.nl/downloads_av/av21.pdf.
105) BW Art. 6:170.
106) Id.

의 명성에 대해 발생한 손해 문제까지 해결되지는 않을 것이다.

바. 소결

인터넷과 이메일 감시에 관한 네덜란드 법의 현황에 대한 설명은 다소 혼란스러운 느낌을 줄 수 있다. 그렇지만 이를 통하여 네덜란드 판례법이 고용관계 내에서 인터넷과 이메일 감시와 관련된 문제를 다루는 방식에 대한 일반적인 결론을 내릴 수는 있을 것이다.

사업장 내 프라이버시에 대해서 규율하는 개별 법령이 네덜란드 내에는 존재하지 않는다. 네덜란드와 유럽의 판례법에 따르면 프라이버시에 대한 기본적인 헌법상의 권리가 적용가능하며 고용관계 내에서의 정보보호에 대한 일반 규정도 적용 가능하다. 그렇지만 판례법에 따를 경우 이러한 권리가 인터넷과 이메일 감시에 있어 중요한 역할을 하지는 않는다. 인터넷과 이메일 감시의 적법성 여부는 일반적으로 부당해고 소송에서 다루어진다. 이러한 소송의 결과는 당해 소송의 사실 관계 및 근로자의 이익과 사용자의 이익간의 비교 형량에 크게 좌우된다. 이런 측면에서 볼 때 비례의 원칙과 보충성의 원칙이 중요한 역할을 하게 된다.[107] 실제 사례에서 사실관계가 갖는 성격을 고려해 볼 때 사용자와 근로자의 이익간 비교형량은 주로 사용자 쪽으로 기울게 된다. 인터넷과 이메일 감시를 통하여 수집된 정보를 바탕으로 한 해고의 적법성 여부를 판단함에 있어 인터넷과 이메일 사용에 관한 회사의 행동규범(code of conduct)의 존재 여부가 결정적이다. 이러한 행동규범의 존재와 내용은 근로자에게 적절히 고지되어야 한다. 그러나 사용자가 만든 행동규범에 의해 명시적으로 금지되지 않았다 할지라도 일부 행위의 경우 이것이 금지되었다는 것을 근로자가 알 수 있었음이 인정될 수도 있다.

프라이버시와 고용관계에 관한 법률에도 불구하고 사용자의 프라이버시 침해 행위에 대해 근로자는 강력한 보호를 받지 못하고 있다. 첫 번째 이유는 근로자의 부정행위(fraudulent behavior)가 사용자에 의한 프라이버시권 침해를 정당화한다는 데 있다. 여기서 '부정'이라 함은 범죄행위뿐만 아니라 회사의 행동규범을 위반한 행위 또한 포함한다.[108] 두 번째 이유는 프라이버시권에 대한

107) Bom, supra note 91.
108) Id.

침해가 인정된다 할지라도 종종 이러한 침해가 정당하다는 판결이 나기 때문이다. 세 번째 이유는 프라이버시권에 대한 침해가 정당하지 않은 것으로 판단된다 할지라도, 이로 인해 법적 책임을 지는 경우는 흔치 않으며, 즉, 근로자가 복직된다든지 증거가 효력을 상실한다든지, 손해배상의 의무가 발생한다든지 하는 결과가 나오지 않는다는 것이다. 프라이버시권 침해의 경우에 대한 법적 책임의 부재가 네덜란드에서의 프라이버시 보호에 있어 가장 큰 흠결이 된다.

4. 양국의 비교

미국 내 프라이버시 보호주의자들이 프라이버시에 대한 유럽의 인권측면에서의 접근방식을 부러운 눈빛으로 바라볼지 몰라도 네덜란드에서의 상황은 이러한 접근방식이 프라이버시에 대한 적절한 보호를 결코 보장하지 못한다는 것을 보여준다. 최소한 사용자의 인터넷과 이메일 감시를 통해 수집된 증거를 바탕으로 한 해고에 있어서는 그러하다. 프라이버시와 정보보호에 관한 규정과 부당해고에 관한 규정이 미국에서보다 네덜란드에서 더 엄격하다 할지라도 실제로 인터넷과 이메일 감시에 대한 근로자의 보호가 더 두터운 것인지는 의문스럽다. 유럽과 네덜란드 판례법의 문제점은 근로자의 프라이버시권 침해가 인정되는 경우에 대하여 적절한 책임을 지우지 않는다는 데 있다. 이런 측면에서 볼 때 최소한 손해배상의 관점에서 보면 미국의 상황이 심지어는 더 낙관적인 것으로 보인다.[109] 미국의 경우 프라이버시 침해가 인정된다면 손해배상이 주어지며 그 금액 또한 유럽에서보다 높을 가능성이 크다.[110] 장기적인 관점에서 보았을 때 미국의 근로자들이 더 나을지 여부는 손해배상액뿐만 아니라 실업급여와 관련된 법령에 달려 있을 것이다. 네덜란드의 경우 미국보다 사회안전망을 잘 갖추고 있긴 하나 이것만으로는 네덜란드의 근로자들이 더 나을 것이라고 판단할 수는 없다. 위에서 언급한 바와 같이 손해배상액이 중요한 요소이긴 하지만 일부 연구에 따를 경우 실업급여의 제공은 직장으로의 재진입을 방해할 수 있다고 한다.[111] 프라이버시권의 침해를 바탕으로 한 해고 이후의 근로자의

109) Supra, pt. I.B.

110) Jacobs, supra note 5, at 219.

111) P. Van Rompuy, De Houdbaarheid van de Europese Welvaartstaat', K.U.Leuven Departement Economie, Leuvense Economische Standpunten (October 2005),

상태에 대해서 좀 더 분명히 알기 위해서는 더 많은 연구가 필요할 것이다. 적절한 배상이 없다면 프라이버시권의 가치 또한 보잘것없는 것이 된다. 따라서 엄청난 액수의 손해배상액을 요구하는 미국식 소송 문화에 기대지 않고서도[112] 프라이버시권이 실질적 의미를 가질 수 있을 정도로 프라이버시권의 침해로 인한 손해에 대해 적절히 배상 받을 수 있도록 하는 것이 중요하다.

프라이버시의 침해가 거의 인정되지 않고 임의로 고용을 해지할 수 있는 사용자의 권한에 대한 적절한 보호책이 존재하지 않는다면 미국에서 프라이버시 침해와 부당해고에 대한 더 많은 액수의 보상은 의미가 없게 된다. 분명한 점은 인터넷과 이메일 감시에 대해 사용자가 갖는 강력한 권한에 대해 현재 미국 내의 보호책은 큰 흠결이 있다는 것이다. 이 중 가장 중요한 흠결은 사용자가 제공한 네트워크상에서 이루어지는 인터넷과 이메일 통신에 있어 근로자가 프라이버시에 대한 정당한 기대를 가질 수 없다는 결론이 너무나도 쉽게 도출된다는 점이다. 결과적으로 감시의 수단과 정도에 대해서는 더 이상의 고려도 하지 않게 된다. 또한 ECPA법의 경우 법에 따른 예외 중 하나가 적용된다면 감시의 범위와 기간과 같은 여타 상황은 전혀 의미가 없어지게 된다. 이런 측면에서 볼 때 미국에서는 감시에 대한 근로자의 동의가 너무 쉽게 간주된다는 점이 지적되어야 할 것이다. 이런 식으로 인터넷과 이메일 감시에 대한 미국식 접근은 사용자의 입지만을 지나치게 강화하게 된다.

고용관계의 해지에 있어서도 동일한 결론이 도출될 수 있다. 사업장 내에서의 프라이버시를 향상시키기 위한 법률안은 투명성에 초점을 맞추고 있다. 인터넷과 이메일에 관한 내부 방침을 갖추고 있다면 당연히 좋은 일이지만, 사용자가 정한 내부 방침 또한 직원의 이익과 함께 비례의 원칙 및 보충성의 원칙을 고려하여 만들어져야 한다. 회사의 내부 방침이 근로자가 갖는 모든 정당한

---

http://www.econ.kuleuven.be/ces/les/LES112.pdf; A. Van der Horst, Structural estimates of equilibrium unemployment in six OECD Economies, CPB Discussion Paper No. 19 (June 2003), http://www.cpb.nl /nl/pub/cpbreeksen/discussie/19/disc19.pdf.

112) See Hartlief, T., 'Leven in een claimcultuur: wie is er bang voor Amerikaanse toestanden?', Nederlands Juristenblad, (Dutch Legal Journal) 2005-16, p.830-834. Undoubtedly there are also big disadvantages to high claims and awards for damages. 네덜란드에서는 이러한 '소송문화'의 장·단점에 관한 논의가 한창이다.

이익을 무효화할 수 있는 사용자의 일방적인 선언이 되어서는 아니 된다. 미국 내의 인터넷과 이메일 감시에 대한 보호책에 있어 근로자의 이익에 대한 고려가 전혀 이루어지지 않는 것과 감시가 시행되고 있는 방식이 주요한 문제가 되고 있다. 프라이버시에 대한 정당한 기대가 없는 경우라 할지라도 사용자가 무엇이든 원하는 대로 할 수 있다는 것은 아니다. 비례의 원칙과 보충성의 원칙의 측면에서뿐만 아니라 공정한 정보처리관행에 관한 일반적인 규정들로부터 근로자를 보호하기 위한 방안들이 도출될 수 있을 것이다. 필터(filter), 차단리스트(block list)나 방화벽(firewall)과 같이 침해 정도가 덜한 감시장비의 적용가능성이나 감시의 수준에 대한 고려가 최소한 필요할 것이다.[113] 또한, 수집한 정보가 사용되고 저장되며 공개되는 방식이 자세히 설명되어야 한다. 이러한 대책들을 통하여 근로자들이 프라이버시에 대한 기대를 다시 가질 수 있을 것이다. 또한 부당해고 사례에서 임의고용의 원칙에 대한 공공질서에 따른 예외가 적용되어 법적 책임이 인정될 수도 있을 것이다. 해결되어야 할 또 다른 문제는 고용관계 내에서의 근로자의 동의의 개념이다. 상대적으로 열위에 있는 근로자의 입장에 균형을 맞추어 주기 위하여 근로자의 동의에 다른 요건들을 추가하여야만 할 것이다. 미국 내에서 더 나은 또는 더 많은 입법이 이루어져야 한다고 주장하는 다른 학자들과 달리[114] 현재의 규정들을 재해석함으로써 사업장 내 프라이버시를 잘 보호할 수 있다고 생각한다.

네덜란드와 미국에서 해결되어야 할 또 다른 문제는 법원에 대한 접근성이다. 높은 소송 비용과 손해배상을 받을 수 있을지 여부에 대한 불확실성이 큰 장벽이 되고 있다. 네덜란드에 있어서는 손해배상액의 한도액이 존재함에 따라 법원에 소를 제기하는 데 있어 또 다른 부담이 되고 있다. 국가정보보호국(NDPA)이 일부 구제책을 제공하고 있긴 하나, 소송에 있어 한도액이 존재함에 따라 손해 전체를 전보 받을 수는 없게 된다. 예를 들어 국가정보보호국이 근로자의 복직을 명할 수는 없다.[115] 또한 분쟁해결이 국가정보보호국의 주요 임

113) [역주] 예컨대 송신된 이메일의 양이나 부서별 인터넷 사용시간을 확인하는 방법에 비해 이메일 내용과 인터넷 접속 사이트를 개인별로 파악하는 방법이 침해의 정도가 훨씬 심한 것이다.

114) See Yung, supra note 35, at 163-222; See also Richman, supra note 72, at 1337-1361.

115) See Personal Data Protection Act, supra note 99, at ch. 10.

무가 아닌 점도 국가정보보호국의 실질적 역할을 감소시키고 있다.[116] 그럼에도 불구하고, 미국에서는 정보보호기관이 공정한 정보처리 방식에 대한 지침을 제공함으로써 일정한 역할을 기대할 수 있으리라 본다. 물론 현 시점에서 미국에서 이러한 역할을 찾아보기는 힘들다.[117]

Ⅲ. 위치추적시스템

1. 개요

위치추적기술을 통하여 새로운 형태의 근로자 감시가 나타나고 있다.[118] 블랙박스(black boxes), 위성위치추적시스템(Global Positioning System)과 RFID 칩에 대한 수많은 광고에서 볼 수 있듯이 이러한 기술과 관련된 산업이 활황을 이루고 있다는 사실은 분명하다. 이러한 기술을 통하여 사용자는 인터넷과 이메일 감시를 활용한 경우보다 근로자의 사생활을 더 깊숙이 파고들 수 있게 된다. 감시의 범위도 회사건물 내에서뿐만 아니라 근무시간 이후까지로 확장될 수 있다. 인터넷과 이메일 감시의 경우에 있어서는 근로자가 가정에 있는 컴퓨터를 통하여 회사 네트워크에 접속하고 이러한 사용이 모니터 되는 경우에만 감시가 가능했었다.

이메일과 인터넷 감시는 근로자가 가상공간 상에서 어디 있는지를 보여줄 수 있었지만 위치추적시스템은 실제 위치를 파악할 수 있게 해준다는 점에서 큰 차이가 있다. 결과적으로 사적 영역과 업무 영역의 구분이 희미해지고, 사용자가 근로자의 모든 생활을 통제할 수 있게 된 것이다.[119] 이렇게 됨으로써 위치

116) See College Bescherming Persoonsgegevens, Uitgangspunten en beleidsregels klachtenbehandeling (http://webcache.googleusercontent.com/search?q=cache:kmkZRyenlzsJ:www.cbpweb.nl/Pages/bel_klachtbehandeling.aspx+College+Bescherming+Persoonsgegevens,+Uitgangspunten+en+beleidsregels+klachtenbehandeling&cd=1&hl=ko&ct=clnk&gl=kr).

117) See Yung, supra note 35, at 217-218. 미국의 경우 노동부(Department of Labor), 고용기회균등위원회(Equal Employment Opportunity Commission), 연방통상위원회(Federal Trade Commission) 등이 사용자들의 감시로부터 근로자를 보호하는 역할을 할 수 있는 기관들이다.

118) [역주] 본 논문에서 'positioning'과 'localization'은 동일한 의미로 사용되고 있다.

추적시스템은 인터넷과 이메일 감시보다 더 심한 침해를 야기할 수 있게 된다. 따라서 이러한 감시의 두 유형을 비교하고 위치추적시스템이 인터넷과 이메일 감시와 동일한 방식으로 다루어 질 수 있는지 또 사용자-근로자간 관계에 어떠한 영향을 미칠 수 있는지를 검토하는 것이 중요하다.

이러한 이슈를 검토하기 전에, 가장 널리 알려진 네 가지 위치추적기술에 대해 간단히 살펴보기로 한다. 이러한 네 가지 기술은 영상감시(video surveillance), RFID 태그, 셀 ID와 GPS이다.[120] 이러한 기술들은 몇몇 다른 목적을 위해서도 전용될 수 있다. 그러나 본 논문에서는 근로자의 위치를 파악하는 기능만을 살펴보기로 한다. 현재까지 밀폐된 근로 공간 내에서는 영상감시와 RFID를 활용하는 것이 가장 적절한 수단이다.[121] 셀 ID와 GPS의 경우 각각 국지적 위치추적과 지구상 위치확인을 활용하게 된다. 영상감시와 RFID도 프라이버시 침해와 관련된 리스크를 수반하게 되며 이를 본 논문 내에서도 검토하게 될 것이다. 그렇지만 본 논문은 회사 건물 밖 및 근무시간 이후에 이루어지는 사용자의 감시를 보다 중점적으로 다루게 될 것이다.

2. 영상감시와 RFID

영상감시는 인터넷과 이메일 감시와 상당 부분 유사하다. 사업장 내에서의 영상감시장비의 설치와 활용에 대해서는 이미 법원에서 몇 차례 다루어진 바 있다. 영상감시가 허용될 수 있기 위해서는 영상감시가 공공장소 혹은 사적 공간에서 행해지는지 여부와 프라이버시에 대한 정당한 기대가 존재하는지 여부 등 두 가지 요건이 갖추어져야 한다.[122][123] 첫 번째 요건의 경우 사업장이 공공장

119) Roberto Fragale Filhot and Joaquim Leonel de Rezende Alvim, Information Technology and Workers' Privacy: Old and New Paradigms, *23 Comp. Lab. L. & Pol'y J 527, 527-532 (Winter 2002).*

120) See James C. White, People Not Places: A Policy Framework for Analyzing Location Privacy Issues, Electronic Privacy Information Center, Spring 2003, http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf.

121) Ronald Leenes & Bert-Jaap Koops, 'Code' and Privacy: Or How Technology is Slowly Eroding Privacy, The Hague, 43 (Asscher Press 2005), available at http://ssrn.com/abstract=661141.

122) R. Gellman, A General Survey of Video Surveillance Law in the United States, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, Reasonable Expectations

소 혹은 사적 공간으로 볼 수 있을 지가 불명확하기 때문에 사업장 내의 프라이버시 관점에서 평가하기가 어려울 것이다.[124] 두 번째 요건의 경우 대체로 사용자가 근로자에게 영상감시에 대해 고지를 했다면 충족되기 어려운 것으로 판단된다.[125] 영상감시를 행하는 이유는 작업절차를 통제하고 근로자의 부정행위에 대한 증거를 수집하기 위해서이다. 그렇지만 영상감시는 사업장 내에서 근로자를 감시하고 추적하기 위해서 사용될 수 있다. 물론 더 큰 규모의 영상감시 네트워크를 활용하는 것도 가능할 것이다. 예를 들면 도로교통위반을 감시하는 영상감시 네트워크 같은 것이 예가 될 수 있다. 그렇지만 사용자가 이러한 기존 시스템에 접속할 권한을 확보하지 못하는 한 현실적으로 이를 활용하기는 힘들 것이다. 또한 그러한 큰 규모의 네트워크를 설치하기에는 비용이 너무 많이 든다. 특히 셀 ID나 GPS와 같은 대체재를 이용할 수 있음을 감안하면 그 비용은 더욱 크게 느껴진다. 셀 ID나 GPS에 연결된 네트워크는 이미 설치가 되어 상업적 사용이 가능한 상태이다.[126] 따라서 위치추적시스템과 관련된 프라이버시에 대한 리스크는 회사 건물 밖에서의 직원의 위치추적과 관련되어 있음을 감안할 때 영상감시기술은 본 논문에서의 논의의 대상에서 제외하기로 한다.

RFID는 각 개별 아이템을 자동으로 확인하기 위하여 사용되는 전자파를 지칭하는 용어인데 현재는 군사, 건강, 소매분야에서 빈번하게 사용되고 있다. 그렇지만 RFID는 사업장 내 출입통제를 위해서 사용되기도 한다.[127] RFID기술은 전자파를 통해 정보를 주고받을 수 있는 태그로 구성된다.[128] 전자파 신호를 수신기가

---

of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, Den Haag: T.C.M. Asser Press (2005).

123) [역주] 우리나라의 경우 근로자참여 및 협력증진에 관한 법률 제20조 제14호에서 노사협의회의 협의사항의 하나로 사업장 내 근로자 감시 설비의 설치를 규정하고 있다.

124) Id.; see also infra pt. I.B.1.

125) Sixto Ortiz Jr., Technology The Boss Uses To Spy on You, Enterprise Security Today, October 11, 2006, http://www.newsfactor.com/story.xhtml?story_id=46809.

126) Adam Theiss, David C.Yen & Cheng-Yaun Ku, Global Positioning Systems: an analysis of applications, current development and future implications, 27 Computer Standards and Interfaces 89, 90 (2005), available at http://www.elsevierscience.com.

127) C.M. Roberts, Radio Frequency Identification (RFID), Computers & Security 25, 18-26 (2005), available at www.sciencedirect.com.

수신하여 추가 처리를 하게 된다.[129] 태그는 칩이나 센서를 담을 수 있다. 수동태그(passive tags)는 리더(reader)에 의해 작동하게 되며, 능동태그(active tags)는 내부에 전력과 함께 원격으로(수 킬로미터까지 가능하지만, 대부분의 경우는 그 이하이다) 신호를 보낼 수 있는 능동수신기(active transmitter)를 담고 있다.[130] 이러한 이유로 인해 RFID는 전 지구적인 위치추적에는 적합하지 않다. 회사 건물 내에서 직원의 위치를 파악하기 위해 RFID를 활용하는 것은 영상감시기술의 경우보다 프라이버시의 침해가 더 심한 것으로 보이지는 않는다. 그렇지만 RFID 기술을 통해서 근로자가 특정 리더(reader)를 통과한 시간이 바로 저장될 수 있으며 이러한 정보가 데이터베이스 내에서 처리되며 이러한 데이터베이스는 다른 데이터베이스들과 연결되어 있을 수 있다. 더욱이 먼 거리에서도 정보가 수집될 수 있고, 직접적인 접촉이 필요 없으므로, 비밀스런 감시의 가능성은 더욱 높아지게 된다.[131] 그럼에도 불구하고 Ronald Leenes와 Bert-Jaap Koops는 현재 이루어지고 있는 RFID 기술의 적용은 전혀 비밀스러운 것으로 보이지 않으며 따라서 프라이버시의 균형을 심하게 깨뜨리지 않는다고 결론을 내리고 있다.[132]

그렇지만 RFID를 계속해서 광범위하게 사용하게 된다면 분명히 각 개인의 프라이버시에 큰 위협이 될 것이다. 예를 들어 개별 RFID 태그에 저장된 정보간의 결합이나 이러한 정보가 데이터베이스에 저장된 외부 정보와 결합되는 경우 이러한 위협이 현실화될 것이다. 이러한 정보의 결합은 각 개인에 대한 정보를 수집하고 감시하는 데 쓰일 수 있다. 그렇지만 회사뿐만 아니라 정부도 각 개인이 소지하는 태그를 뒤따라감으로써 각 개인을 추적할 수 있다. 각 태그는 개별 식별번호를 가지고 있기 때문에 개인에 대한 추적이 가능해진다.[133] RFID가 프라이버시에 대한 위협이 될지 여부 및 그 정도는 RFID 태그가

128) Id.
129) Leenes, supra note 96, at 42.
130) Id.
131) J. Verwer, 'Werknemers en RFID, in Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, 73, 80 Nederlandse Vereniging voor Informatietechnologie en Recht (Den Haag: Elsevier Juridisch 2005), available at http://www.nvvir.nl/doc/rfid-tekst.pdf; see also M. Jeffery, Information Technology and Workers' Privacy: Introduction, 23 Computer Labor L. and Pol'y J. 251, 251-280.
132) Leenes, supra note 96, at 44.

어떻게, 또 얼마나 오랜 기간 동안 이용될 지와 누가 이를 해독하게 될지 및 어떤 상황에서 태그가 이용되는지에 달려있다.[134]

현재까지 사용자는 회사 건물 자체에 대한 출입통제와 건물 내에서의 출입통제에 있어 RFID 태그를 활용하는 데 관심을 가져왔다. 각 근로자의 카드에 포함된 RFID 태그는 회사 건물 내 특정 장소에 근로자의 출입을 허용하거나 이를 거부하는 역할을 하였다. 또한 근로자가 통과한 모든 RFID 리더를 확인함으로써 근로자가 회사 내에서 어디를 다녔는지를 추적할 수 있었다. 이는 사내 연애를 찾아내는 데 사용되는 것과 같이 프라이버시를 침해할 가능성이 있다. 그러나 이는 영상감시, 이메일 감시나 혹은 회사 내 소문을 통해서도 쉽게 찾아낼 수 있는 것이기도 하다. RFID 태그가 갖는 또 다른 흥미로운 용도는 회사 자산을 보호하는 것이다. 근로자뿐만 아니라 회사 자산에도 태그를 달 수 있다. 만일 RFID 태그가 리더가 부착된 문을 통과하게 되면 기록이 남게 된다. 근로자가 소지하고 있는 개인 카드를 함께 활용함으로써 누가 어떤 회사 재산을 가지고 회사 건물 밖을 나섰는지를 찾아낼 수 있다. 위에서 언급한 바와 같이 회사 건물 밖에서 사용자가 근로자를 추적하기 위해서는 다른 기술들을 사용하는 것이 더 적합할 것이다.

3. 셀 ID와 GPS

셀 ID와 GPS는 동일한 원리로 작동하지만 어떤 면에서는 정반대이기도 하다. 셀 ID의 경우 네트워크에 기반을 둔 시스템을 통하여 이동전화의 위치를 찾을 수 있게 된다.[135] 네트워크가 어느 지역에 이동전화가 위치하고 있는지를 알려주게 되는 것이다.[136] GPS의 경우 위성이 휴대용 단말기의 위치를 알려주게 된다.[137] 네트워크에 기반을 둔 위치정보와 달리, GPS의 위성 네트워크는 그 장비의 위치는 알 수 없다. GPS 장비 자체가 위성을 기반으로 하여 위치를

133) Id. at 45.
134) Id. at 46.
135) See Location Management in GSM, http://www.volny.cz/drd/gsm/ GSMLocationManagement.html
136) Leenes, supra note 96, at 29.
137) See Garmin, Garmin: GPS for Beginners, http://www8.garmin.com/aboutGPS/manual.html

계산하게 된다. 이동전화나 (GPS 트랜스시버 내의) 무선송신기, 매 분단위로 좌표를 저장하는 디스크와 프로그램(GPS 리코더라고 불림)과 결합하여 GPS는 위치정보를 제3자에게 제공할 수 있다.[138] GPS를 통한 정확한 위치측정은 삼각측량 혹은 GPS 휴대용 수신기와 3개 이상의 GPS 위성간의 거리를 파악하여 지구상 특정 위치를 찾아내는 과정을 통해 가능하게 된다.[139] 삼각측량은 또한 셀 ID를 통한 위치파악을 향상하는 데도 활용된다.[140] 이동전화는 셀 ID에서 활용될 수 있을 뿐만 아니라 GPS 발신기(GPS beacon)와 함께 이용될 수 있다.[141] 또한 PDA가 이러한 GPS 발신기와의 교신을 위해 널리 이용되는 휴대장비이기도 하다.

인터넷과 이메일 감시의 경우와 마찬가지로 사용자의 위치추적기술의 활용 또한 손쉽게 정당화될 수 있다. 핸드폰, PDA와 GPS기술을 결합함으로써 사용자는 현장에서 일하는 근로자들과 통신할 수 있는 뛰어난 장비를 갖출 수 있게 된다. 택시사업을 예로 들어보자. 위치추적기술은 여러 대의 택시를 최대한 효율적으로 배차하는 데 활용될 수 있다. 또한 도난차량의 위치를 파악하는 데 도움을 줄 수도 있다. 또한 자동차 절도범들도 추적이 가능한 차를 훔치는 것을 주저하게 될 것이다. 자동차 소유자와 택시 기사들은 위치추적기술을 활용함으로써 더 안전하다고 느끼게 된다. 더욱이 GPS 장비를 통해 수집한 정보를 바탕으로 하여 교통량을 분산함으로써 교통정체를 피할 수 있을 것이다. 그렇지만 이러한 위치추적기술을 통하여 사용자는 근로자의 모든 움직임을 매일 24시간 내내 추적하고 통제할 수 있게 된다. 위험한 점은 근로와 관계된 정보와 사생활에 관계된 정보간에 존재하는 모호한 경계가 희미해질 수 있다는 점이다. 인터넷과 이메일 감시의 경우보다 위치추적기술은 더 넓은 규모의 통제를 가능하게 해 준다. 실제 근로자는 사용자의 시야에서 전혀 벗어날 수 없게 된다.

근로자 입장에서는 본인의 사적인 시간에는 사용자가 제공한 장비를 사용하

138) Leenes, supra note 121, at 29.
139) Theiss, supra note 126, at 91.
140) See Leenes, supra note 121, at 29 (stating that the same goes for Cell ID where the localization is enhanced by triangulation using the speed and angle with which a mobile phone enters or leaves a cell and comparing signals received by various cells at the same time).
141) Theiss, supra note 126, at 98.

지 않음으로써 감시를 피할 수 있을 것이다.[142] 가능하다면 위치추적장비를 꺼놓는 것도 한 방법이 될 수 있다. 사용자는 근로자가 이동전화나 PDA를 사적인 목적을 위해 사용해서는 안 된다고 주장할 수도 있다. 근로자는 퇴근 후에는 이러한 장비들을 집에 둠으로써 추적을 피할 수도 있다. 그렇지만 대체로 사용자는 근로자들이 이러한 장비를 사용할 수 있게 해 줌으로써 더 큰 이익을 보게 된다. 사용자가 근로자와 연락을 취하기가 쉬워지기 때문이다. 예를 들어 회사에서 제공한 이동전화를 사적인 용도로 사용할 수 있게 해주면 회사 입장에서는 근로자가 공식적으로 업무를 마친 이후에도 업무와 관련된 문제 해결을 위하여 근로자와 연락을 취할 수 있게 된다. 이러한 기술의 발전으로 인하여 오전 9시에서 오후 5시라는 근무시간은 포기될 수 밖에 없다. 이러한 고정된 근무시간은 새로운 경제 체계 내에서는 더 이상 바람직한 것이 아니기도 하다. 회사에서 제공하는 차량의 경우 근로자가 근무시간이 지났다고 하여 이를 주차장에 내버려 두기는 더 힘들어진다. 대부분의 근로자에게 있어 회사 차와 별개로 자기 차를 소유하는 것은 유지비용이 너무 많이 들기 때문이다. 따라서 실제로는 많은 근로자들이 본인의 여가 시간에도 위치추적이 가능한 장비들을 가지고 다니게 된다. 위치추적기능을 꺼놓을 수 없는 경우라면 인터넷과 이메일 감시보다 위치추적을 통한 감시의 경우에 더 큰 사생활 침해 리스크가 상존하게 된다. 인터넷과 이메일 감시의 경우와 유사하게 사후적 통제가 이루어질 위험성도 있게 된다. 대부분의 GPS 장비는 저장된 위치정보를 복구할 수 있는 기능을 가지고 있다. 따라서 실시간으로뿐만 아니라 어떤 사건이 발생한 후에도 사용자는 필요한 정보를 빼낼 수 있게 된다.

인터넷과 이메일 감시 기술과 마찬가지로 위치추적기술은 어떤 인물에 대한 시간과 장소 정보만을 제공하게 된다. 어느 시간대에 어느 장소에 있었는지는 알 수 있어도 왜 그 시간에 거기에 있는지는 파악할 수 없다. 근로자가 회사 차량을 가지고 출입이 금지된 홍등가에 들어가는 경우 그 근로자가 위법행위를 하고 있을 수도 있지만 단순히 길을 잃었을 수도 있다.[143] 또한 위치추적기술

142) See generally Xora, GPS Time Track for Workers; Track and Manage Your Workers in Real Time, http://xora1.securesites.net/timetrack/productinfo.html (last visited Oct. 15, 2007).

143) Id.

은 일반적으로 당해 장비의 위치만을 알려주게 되며 금지구역에 들어가는 근로자의 위치를 알려주는 것은 아니다. 예를 들어, 근로자의 차가 도난 되었다면, 위치추적기술은 잘못된 정보를 제공하게 될 것이다. GPS와 같은 기술을 통하여 취득한 위치정보는 근로자를 해고할 이유를 찾는 데 활용될 수도 있다. 특히 사용자가 어떤 이유를 찾아서라도 근로자를 해고하고자 할 때 이용될 수 있다.[144] 기술, 특히 발전 단계에 있는 기술이라면 단점이 있기 마련이다. 근로자의 입장에서는 위치추적장비가 오작동했다는 사실을 증명하기가 힘들다. 근로자가 알지 못한 상태에서 위치추적장비가 누군가에 의해 조정되었거나 결과가 조작되었을 수도 있다.

GPS장비의 위치를 결정하는 데 사용되는 삼각측량은 밀집 지역에서는 제대로 작동하기 힘들다. 강렬한 햇빛이 장비의 오작동을 일으킬 수도 있다.[145] 이외에도 대기의 영향, 다중경로에 의한 영향(multipath effects), 스푸핑(spoofing), 고의오차신호(selective availability)와 같은 다양한 원인들이 GPS의 오작동에 영향을 미칠 수 있다.[146] GPS 장비 오작동의 경우뿐만 아니라 고의적으로 장비의 정확도를 떨어뜨리는 경우도 있을 수 있다.[147] 따라서 사용자는 GPS 기술을 통해 수집한 정보를 항상 신뢰할 수는 없다는 점을 명심해야 한다.

4. 근로자의 위치추적에 적용되는 인터넷 및 이메일 감시 관련 법률

가. 미국

2001년에 발의된 바는 있으나 위치 관련 프라이버시에 대해서 미국 내에는 특별한 법률이 없다.[148] 연방 법률 Title 18, Section 2702는 고객의 통신 내용

144) Yung, supra note 35, at 180.

145) Steve Bush, Solar Flares Can Cause GPS Malfunction, Say Researchers, Electronics Weekly, Oct. 13, 2006.

146) Greg Pendleton, The Fundamentals of GPS, Directions Magazine (July 16, 2002), http://www.directionsmag.com/article.php?article id=228&trv=1.

147) Bob Brewin, Homemade GPS jammers raise concerns, http://www.computerworld.com/s/article /77702/ Homemade_GPS_jammers_raise_concerns.

148) Location Privacy Protection Act of 2001, S. 1164, 107th Cong. 1st Sess. (1999). 동법은 소비자의 프라이버시 보호가 목적이었기 때문에 근로자들에게

이나 기록의 공개에 적용되는 법률의 기본 골격을 제공한다.[149] 본 법률은 전자통신서비스나 원격 컴퓨터 서비스를 제공하는 개인이나 업체는 통신 내용이나 위치정보와 같이 가입자와 관련된 기타 정보를 고의적으로 공개하지 못하도록 하고 있다.[150] 그렇지만 고객이나 가입자로부터 적법한 동의를 받은 경우 예외가 적용되기 때문에 본 법률은 폭넓은 보호를 제공하지는 못한다.

통신 내용이나 기록과 관련된 연방법률 이외에 section II.B에 규정된 일반 규정이 위치추적기술에 적용된다. 인터넷과 이메일감시를 재산권을 바탕으로 하여 접근하는 방식은 위치추적기술에도 적용되므로 인터넷과 이메일감시에 관한 내용이 도움이 될 수 있다. 근로자가 프라이버시에 대한 정당한 기대를 가지고 있었는지 여부가 해결되어야 할 중요한 이슈가 된다.

근로자가 프라이버시에 대한 정당한 기대를 가졌는지 여부에 영향을 미치는 세 가지 중요한 인자들은 (ⅰ) 정보의 성격, (ⅱ) 사용된 기술, (ⅲ) 사적인 정보를 제3자에게 자발적으로 넘겼는지 여부가 된다. 정보의 성격의 경우 셀 ID나 GPS는 단지 내용이 채워져 있지 않은 정보만을 제공한다는 점이 부각될 수 있다. 그렇지만 셀 ID와 GPS 정보는 한 사람의 개인 생활에 대한 많은 양의 정보를 공개할 수 있다. 워싱턴 대법원은 Jackson 사건에서 GPS 장비가 병원, 카지노, 스트립바나 노동집회와 같은 장소에 갔는지 여부에 대한 자세한 정보를 제공할 수 있는 가능성을 인정한 바 있다.[151] 신기술의 사생활 침해 가능성을 정부가 인정하면서 위에서 언급한 바 있는 Kyllo 규정(the Kyllo rule)이 생겨나게 되었다. 본 규정에 따를 경우 정부는 헌법상 보장된 사적인 정보나 장소를 영장 없이 수색하기 위해서는 기술의 도움을 받지 않고 인간의 감각기관을 활용하여야 하며, 필요한 경우라도 일반적으로 널리 이용되고 있는 보편적 기술만을 활용하여야 한다.[152] Kyllo 규정에 따를 경우 프라이버시에 대한 정당한 기대가 있었는지 여부는 보통의 시각 감시에 의해서도 당해 정보에 대한 수집이 가능했느냐에 달려 있다.[153] 매우 드문 경우이겠지만 동일한 정보가 시

적용될 수 있을지는 의문이다. 동법에 따르면 통지가 요구되고 위치정보를 이용하거나 제3자에 공개하는데도 일정한 제한을 두었다.

149) *18 U.S.C. 2702* (2006) (소비자의 통신・기록 등의 자발적인 공개에 관한 것이다).

150) Id.

151) *Washington v. Jackson, 76 P.3d 217, 223 (Wash. 2003).*

152) *Kyllo v. United States, 533 U.S. 27, 34 (2001).*

각 감시에 의해서 수집될 수도 있을 것이다. 전자추적장비는 시각 감시에 의한 경우와 비교했을 때 장기간 동안의 정보 수집을 가능하게 해 준다. 예를 들어 GPS 장비를 활용한다면 한 달 동안도 감시가 가능하겠지만, 사람이 직접 감시한다면 한 달 동안 24시간 내내 감시한다는 것은 상상하기 힘들다.

Jackson 사건에서 법원은 위치정보에 있어 사생활에 대한 정당한 기대를 가질 수 있음을 명시적으로 인정하면서 GPS 감시가 단순한 시각 감시와 동일하게 취급될 수 없다고 하였다. 그렇지만 'United States v. McIver' 사건에서는 추적장비가 차의 실내가 아닌 실외에 장착되었으므로 사생활 침해가 없다는 판결을 내린 바 있다.[154] 본 사례에서는 위치정보의 침해여부가 아니라 추적장치의 설치장소에 따라 결론이 난 것이다. 차량이나 이동전화와 같은 개인의 소유물 내에 위치추적장치를 설치할 가능성이 높아져 가는 기술적·사회적 경향을 고려한다면 Jackson 사례에서의 판결 내용이 더 큰 힘을 얻게 될 것으로 보인다.[155] 그렇지만 일반적인 고용관계를 고려한다면 이는 개인의 사생활 보호를 전혀 보장할 수 없을 것이다. 왜냐하면 사용자들은 근로자에 대한 고지를 통하여 사생활에 대한 기대를 손쉽게 무효화할 수 있을 것이기 때문이다. 사법기관은 GPS 감시를 위해서 영장을 받아야 하겠지만 사용자는 계약을 통하여 동일한 GPS 감시를 행할 수 있다. 근로자에게 이러한 감시가 고용계약의 조건임을 고지만 하면 되는 것이다.

그렇지만 판례법에 따를 경우 사적인 관계에서는 사생활에 대한 기대의 존재여부가 순전히 제3자에게 사적인 정보를 자발적으로 넘겼는지에 따라 결정된다. Smith 사건에서 법원은 개인이 집에서 사적으로 통화한 전화번호에 대하여 사생활에 대한 정당한 기대를 가질 수 없다고 보았다. 이에 따르면 집에서 전화를 건 개인이 이러한 전화번호를 제3자인 전화 회사에 자발적으로 넘김으로써 이러한 번호에 있어서 사생활에 대한 정당한 기대를 제거한 것으로 본 것이다.[156]

---

153) Caldwell, supra note 25, at 67.
154) *186 F.3d 1119 (9th Cir. 1999).*
155) Caldwell, supra note 25, at 70.
156) *Smith v. Maryland, 442 U.S. 735, 742 (1979)*; 반면 일부 주법원들은 전화회사에 자발적으로 넘긴 것으로 볼 수 없다고 보았다(Caldwell supra note 25, at 65). 이 경우 개인들은 자신이 건 전화번호에 관한 프라이버시에 있어 정당한 기대를 갖는 것으로 인정될 수 있다. Id.

사적인 공간에서의 핸드폰에 의한 통신에 있어서는 어느 정도 사생활에 대한 기대가 인정이 된다.[157] 그렇지만 위에서 설명한 바와 같이 이러한 기대에 대한 권리는 고용관계 내에서 손쉽게 포기될 수 있다. 예를 들어 근로자가 이동전화나 PDA와 같은 회사 자산을 사용하는 경우 모든 프라이버시권을 포기하는 것이 된다. 근로자는 회사 자산을 사용하는 경우 프라이버시에 대한 정당한 기대를 더 이상 가질 수 없게 되는 것이다. 근로자가 어느 정도 사생활에 대한 정당한 기대를 가지는 경우라 할지라도 사용자의 자산을 부적절하거나 업무에 관계없이 사용하는 것을 방지하고자 하는 사용자의 적법한 이익이 아마도 근로자의 이익보다 우선하는 것으로 판단될 것이다.

사용자가 근로자들에게 위치추적시스템이 이용되고 있음을 고지할 의무를 질 수도 있다. 인터넷과 이메일에 대한 판례법은 사용자의 고지의무에 대한 사항을 설명하고 있다. 그렇지만 사용자가 실제로 인터넷과 이메일 감시에 관하여 근로자에게 고지할 의무를 부담하는가에 대해서는 불명확하다. Smith 사건에 따르면 근로자에 대한 고지가 불필요하다는 결론에 도달하게 된다.[158] 그렇지만 사용자가 근로자에게 셀 ID나 GPS의 사용에 대해 고지할 의무를 져야 하는 이유를 설명할 수 있는 두 가지 논리가 있다. 첫 번째로 근로자에 대한 위치추적은 인터넷과 이메일의 사용이나 통제와는 달리 사회 내에서 일반적으로 인정되고 있지 않다. 두 번째로 위치추적은 사용자의 영역을 벗어나서 행해지기 때문에 이는 사용자의 근로자에 대한 통제범위를 넘어서는 것이므로 고지의무가 생겨날 수 있다. 이러한 접근 방식이 위치추적기술의 사용에 대한 미국 판례법에서 채택되어 왔다.[159] 회사차량을 사용하는 경우 위치추적장비에 의해 감시를 받게 됨을 회사 방침에 따라 근로자에게 고지하였다면 당해 근로자는 프라이버시에 대한 정당한 기대를 가질 수 없게 된다. 동일한 논리가 이동전화나 PDA를 사적인 용도로 사용하는 것에 관한 회사 방침에도 적용된다. 이는 이동전화나 PDA

157) Caldwell, supra note 25, at 57.

158) *Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).*

159) *People v. Zichovic, 94 Cal. App. 4th 944 (Cal. App. 6th Dist. 2001); Osburn v. Nevada, 44 P.3d 523 (Nev. 2002); State v. Meredith, 337 Ore. 299 (2004)*; see also Nixon Peabody LLP, Employers Tracking Device Does Not Violate Employee's Privacy Rights, Employment Law Alert (2005), available http://www.nixonpeabody.com/linked_media/publications/ELA_01012005.pdf.

가 위치추적을 위한 장비로 사용되느냐에 관계없이 적용되는 것이다. 위치추적 기술에 적용되는 이러한 논리는 인터넷과 이메일감시에 적용되는 것과 동일하다. 인터넷과 이메일을 위하여 회사 장비를 이용하는 경우 당해 근로자는 프라이버시권을 포기하는 것이 되며, 특히 근로자에게 감시에 대해 고지를 해야 한다는 행동규범(code of conduct)이 있는 경우라면 더더욱 그러하다.[160]

그러나 근로자가 고지를 받은 경우라 할지라도 사용자의 행동규범이 반드시 합리적인 것으로 되는 것은 아니다. 판례법에 따르면 위치추적기술과 관련하여 이러한 기술을 사용하는 데 대한 근로자의 동의가 당연히 간주되는 것처럼 보인다.[161] 사용자에 비해 상대적으로 열위에 있는 근로자의 입장도 합리성 여부의 판단에 있어 한 고려요소가 되어야 한다. 근로자의 위치추적과 관련된 사실관계가 사용자의 위치추적기술 사용의 적법성 여부를 판단하는 데 있어 일정한 역할을 할 수 있는지 또한 의심스럽다. 이런 측면에서 본다면 사용자의 회사차량 추적에 대한 Oregon 대법원의 평결이 어느 정도 희망을 준다. 송신기(transmitter)가 발신하는 정보를 통한 사용자의 감시로부터 근로자가 자신의 위치나 업무관련 활동을 감출 수 없음을 법원이 전원일치로 판결하였다 할지라도, 법원은 또한 송신기가 오직 차량의 위치만을 알려주고 다른 정보는 알려주지 않았음을 강조하였다.[162] 법원은 합리성의 판단에 있어 고려되어야 할 두 가지 중요한 사실 관계를 언급하였다. 우선 법원은 위치추적기술이 업무관련 활동에 대해 이용되어야 함을 명시적으로 언급하였다. 따라서 만일 근로자가 자신의 여가 시간에 회사 차량을 이용하는 데 대해 추적이 이루어졌다면 본 사안의 결론은 달라졌을 수 있다. 물론 이는 사용자가 회사 차량의 사적 이용을 허용했을 경우에 한정될 것이다.[163] 두 번째로 송신기가 발신하는 정보의 종류가 고려된다. 송신기는 근로자의 위치를 알려줄 수 있으나, 다른 정보 또한 사용자에게 제공되었느냐가 문제가 된다.

Ortega 사례와는 달리 Oregon 대법원은 프라이버시에 대한 정당한 기대를

160) See *Zichovic, 94 Cal. App. 4th 944*. 개인은 경찰관이 차량에 추적장치를 부착한 경우에도 프라이버시에 관한 합리적 기대가 인정되지 않는다고 한다.; see also Osburn, 44 P.3d 523; see also Nixon Peabody LLP, supra note 159.

161) See Nixon Peabody LLP, supra note 159.

162) *Meredith, 337 Ore. 299*.

163) 차량의 위치정보 외에 회사 재산의 부적절한 개인적 사용에 대한 정보를 수집할 수 있다.

찾기 전에 주변 사실 관계의 합리성 여부를 고려하였다.[164] 이는 미국 내 사업장에서의 프라이버시에 대한 좀 더 균형 잡힌 접근을 위한 첫 번째 조치가 취해진 것이기도 하다. 두 번째 심사는 프라이버시에 대한 기대와 관련이 있는 것이 아니라 사용자에 의한 감시의 적절성 여부이다. 이러한 두 번째 심사는 위치추적시스템에만 적용될 것이 아니라 사용자에 의한 근로자 감시를 위하여 도입되었거나 도입될 모든 기술에 대해 적용되어야 한다. 만일 인터넷과 이메일 감시에 대한 일반적인 접근 방식이 위치추적시스템에도 적용이 된다면 프라이버시는 전혀 의미 없는 개념으로 전락될 것이다. 사용자는 사업장 밖에서나 업무시간 이외에도 근로자를 감시할 권리를 가지게 될 것이다. 이 때 사용자는 단순히 근로자가 사용자가 제공한 자산을 이용하고 있음을 근거로 들면 된다. 이렇게 되면 근로자는 사생활에 대한 어떠한 기대도 가질 수 없게 되기 때문이다. 근로자에게 지속적인 위치감시가 이루어질 가능성을 고지함으로써 사용자의 입지를 더욱 강화할 수도 있다. 공정한 정보 처리에 관한 어떠한 규정도 미국 내에는 존재하지 않는다. 위치추적시스템에 관한 상세한 정보가 근로자에게 제공되고 이러한 정보를 바탕으로 위치추적장치를 정지시킬 수 있다면 근로자가 어느 정도 안심할 수 있을 것이다. 그렇지만 사용자는 본인의 재산권을 근거로 하여 근로자가 장비를 정지시키는 것을 막을 수도 있다. 심지어는 근로자의 근무시간 이후에도 위치추적장비를 끌 수 없도록 할 수 있는 것이다.

사실관계가 프라이버시에 대한 보호를 향상시킬 수 있느냐 여부가 임의고용의 원칙(the employment at will doctrine)에 대하여 프라이버시권 위반을 근거로 하여 공공 정책에 따른 예외를 인정할 것인지 여부에 있어 결정적인 역할을 하게 된다. 이러한 프라이버시권 위반을 성공적으로 주장할 수 있는 가능성을 높이게 되면 소송과 관련된 문제들을 줄일 수 있게 될 것이다.

나. 네덜란드

네덜란드의 경우 교통과 위치정보의 처리에 관한 구체적인 규정이 네덜란드 통신법(the Dutch Telecommunications Act)에 포함되어 있다.[165] 본 규정은

164) *O'Conner, 480 U.S. 709 (1987).*

165) Telecommunicatiewet: Wet van 19 oktober 1998, Stb. 1998, 610; 영역된 자료로는 Peter V. Eijsvoogel en Hendrik Jan De Ru, A practical introduction to the

전자통신분야에서의 개인정보 처리와 사생활 보호에 관한 EU 지침(European Directive 2002/58/EC)에 그 기원을 두고 있다.[166] 네덜란드통신법 11.5와 11.5a조에 따르면 일반 대중에게 전자통신네트워크와 서비스를 제공하는 사업자는 이용자의 동의에 의해서만 교통과 위치정보를 처리할 수 있다. 다만, 요금정산 목적으로 필요하거나 정보가 익명으로 만들어졌을 경우에는 예외로 한다.[167] 본 법령은 고용관계에는 적용되지 아니할 수 있다. 우선 근로자는 사용자의 추적에 대하여 자신의 자유의사에 따라 동의 여부를 결정하지 못할 수 있다. 더욱이 네덜란드통신법상 규정이 일반 대중에게 제공되는 네트워크와 서비스에 대해서만 적용되므로, 사용자는 사적인 위치추적시스템을 활용함으로써 본 규정을 손쉽게 회피할 수 있다.

네덜란드통신법상 규정 이외에는 위치정보의 활용과 관련된 구체적인 규정이 네덜란드 내에는 존재하지 않는다. 따라서 위치정보의 활용과 관련된 분쟁의 경우 제Ⅱ장. 3.에서 설명한 바 있는 네덜란드의 현행 법령에 따라 해결되어야 한다.

현재까지 사용자가 GPS를 활용하여 회사 차량을 이용하는 근로자를 추적한 것과 관련하여 알려진 네덜란드 내 사례는 한 건이다. 본 사례는 공식적인 문건으로 소개된 바는 없으나, 한 로펌의 웹사이트에서 구체적인 내용을 확인할 수 있다.[168] 이에 따르면 GPS 장비상의 정보가 근로자의 근무시간등록을 확인할 목적으로 이용되었다. 당해 근로자는 본인이 근무시간 동안 사용하는 회사 차량이 운전시간과 운전장소를 등록하는 GPS 시스템을 장착하고 있음을 인지하고 있었다. 당해 근로자가 등록된 근무시간상의 숫자가 차이가 나는 데 대해 이유를 충분히 설명하지 못하였기 때문에 사용자는 고용관계를 해지하기로 결정하였다. 재판부는 GPS 시스템을 통하여 수집한 정보는 증거력이 인정되고 이에 기초한 고용해지는 정당하다고 보았다. 이에는 근로자가 GPS 장비와 그 기능에 대해 알고 있었으므로 근로자가 예상치 못한 비밀감시가 존재하지 않았다는 점이 고려되었다.

---

telecommunications laws of the Netherlands, Dutch Telecommunications Law (2001).

166) Id.

167) Id.

168) See Fillet Advocaten, De rijdende prikklok, http://www.fillet.nl/archief/0703.htm; http://www. kamerbeekfillet.nl/ nieuws-02032005-Derijdendeprikklok.asp.

GPS 장비는 근무일의 일정 시간 동안 근로자의 위치와 관련된 정보만을 등록하였다. 따라서 본 장비는 시계와 같은 것에 불과하였다. 이와 같은 시계는 사용자가 취할 수 있는 일반적인 통제장치에 불과한 것이다. 또한 당해 차량이 회사 차량이었으므로 사용자가 근무 시간 동안 차량의 이용에 대해 감시한 것이 정당화 될 수 있다.

네덜란드의 사례는 미국에서 인터넷과 이메일 감시에 대해 접근하는 방식과 동일한 방식을 적용한 것처럼 보인다. 본 사례의 쟁점은 부당해고였으며 판단은 주로 사실관계를 바탕으로 도출되었다. 근로자가 감시에 대해 알고 있었는지 여부가 중요하다. 또한, GPS 장비를 통해 수집되는 정보의 종류와 감시가 이루어졌던 시간대가 중요하다. 이러한 고려사항들은 이익의 균형과 보충성의 원칙과 관련이 있다. 또한 본 사례에 있어 사실관계에 대한 평가와 양자간 이익형량의 결과 사용자가 승소하게 되었다. 또한 형평의 관점에서 볼 때 이러한 결과는 근로자의 사기적인 행위에 따른 것일 수도 있다. 그러나 이는 사기적인 행위가 있었다는 사실이 기발생한 사생활의 침해를 정당화할 수 있느냐는 의문을 불러일으킨다. 사용자에게 유리한 판결이 나왔으므로 사생활에 대한 침해가 전혀 의미가 없었는지에 대해서는 결론을 내릴 수 없게 되었다. 사생활의 침해는 이러한 판결에 영향을 미치지 않았기 때문이다. 인터넷과 이메일감시에서와 마찬가지로 위치추적 사례에서도 최소한도의 책임만이 발생하게 된다면, 사업장 내에서 사생활의 지위가 약화되는 것은 불가피하다.

Ⅳ. 결어

상기의 분석 내용에서 볼 수 있듯이 네덜란드는 물론 미국 내에서도 인터넷과 이메일감시 관련 법령은 근로자의 사생활에 대해 적절한 보호를 제공하지 못한다. 이는 아마도 위치추적시스템과 관련된 법령도 마찬가지 일 것이다. 사례 분석에 따를 경우 ICT는 사용자와 근로자간의 힘의 균형에 있어 사용자 쪽으로 기우는 경향이 있다. 네덜란드에서는 적절한 법률이 제정되어는 있으나 실제적인 적용에 있어서는 자주 무시되는 것으로 보인다. 미국의 법률 체계 내에서 해당 법령은 네덜란드의 법령에 비해 약한 정도의 보호만을 제공하고 있다. 미국의 판례법은 근로자가 사생활 침해에 대해 고지를 받은 한 근로자의

사생활에 대한 침해를 강력히 허용하는 경향이 있다. 상기 제Ⅲ장 4.에서 설명한 바와 같이 근로자의 보호를 위하여 몇몇 변화들이 필요하다. 사용자와 근로자간 적절한 힘의 균형을 되찾기 위해서 근로자에 대한 보호가 필요하다. 본 결론은 네덜란드는 물론 미국에도 동일하게 적용된다.

그러나 근로자 감시에 대한 미국방식의 접근이 정당하다는 주장도 일면 가능하다. 왜 사용자가 근로자의 행동을 감시하는 데 대하여 광범위한 권리를 가질 수 없단 말인가? 사용자는 근로자의 행동에 대하여 책임을 져야 할 수 있으며, 사용자는 근로자의 어떤 활동에 대하여 급여가 지급되고 있는지를 확인할 수 있어야 한다. 더구나 근로자는 사용자의 자산을 이용하고 있으므로 사용자가 본 자산에 대한 이용을 결정하고 통제할 수 있어야 한다. 사업장 내에서 사생활 보호가 필요한지 자체에 대하여 의문이 들 수 있다. 근로자가 사용자의 자산을 사적인 목적을 위하여 이용하지 않는다면 본 자산에 대한 감시가 근로자의 사적 영역을 침범할 수 없을 것이다. 그렇지만 근로자의 프라이버시권보다 사용자의 재산권을 우선시 하는 견해에는 몇 가지 흠결이 존재한다. 우선 근로자를 지속적으로 감시하는 경우 이는 근로자의 존엄성에 대한 침해가 될 수 있다. 이는 감시가 근로자의 사생활 영역에 대해서 이루어지는지 여부와는 무관한 것이다. 더욱이 새로운 감시기술들은 사업장이나 근로자의 업무 관련 활동에 대해서만 한정적으로 적용되지 아니한다.

이는 두 번째 이유와 연결된다. 사용자의 자산에 대한 사적인 이용을 금지하는 것은 미국이나 네덜란드 내의 신경제체계의 현실과 맞지 않는다. 사용자의 자산을 사적으로 이용할 수 있게 해주는 것은 흔히 복리후생(fringe benefit)의 일종으로 간주되기 때문이다. 근로자는 회사 자산의 사적인 이용에 대한 회사의 관대함을 기대하게 되고, 사용자 또한 근로자가 오전 9시에서 오후 5시까지만 근무하겠다는 고정관념을 깨기 위해서 이를 장려하기도 한다. 많은 회사들이 근로자들에게 컴퓨터나 핸드폰을 제공하고 사적인 이용을 허락해 주고 있다. 사용자의 입장에서 추가적인 이익은 365일 24시간 내내 근로자에게 업무 목적으로 연락을 취할 수 있다는 점이다. 사용자가 근로자의 행동을 감시할 강력한 권리를 갖고 있다 할지라도 이러한 권리가 근무시간과 회사 밖으로까지 적용될 수 있느냐에 대해서는 의문의 여지가 남는다. 사용자가 근로자의 사적 생활에 대해 캐고 다닐 수 있는 권리를 가져야 하는가? 더욱이 근로자의 여가 시간의

행동에 대해 회사가 책임을 묻는 것이 정당화 될 수 있는가? 이러한 점에서 David Phillips는 미국의 경우에 대하여 다음과 같은 점을 지적한다: 반대되는 공공규정이 없는 한 민간 기업체의 근로자나 소방관 모두 다 근무 시간 외의 활동에 대해서는 자유를 갖는다. 그러한 자유를 금지하는 공공정책은 각 주의 헌법상에 규정된 사생활 보호규정의 형태나 명시적인 입법에 의해서만 가능한 것이다. 몇몇 주의 경우 임의고용의 원칙에 대한 예외가 있긴 하지만 이는 비교적 드문 경우이다.[169]

인터넷과 이메일 감시에 대한 네덜란드 판례법에 의하면 근로자의 위법행위를 발견한 경우 그것이 심지어 근무시간 이후에 일어났다 할지라도 사용자의 사생활 침해가 정당하다는 결론에 이르게 될 수 있다. 만일 이러한 사생활 침해가 정당하지 않은 것으로 간주되는 경우라도 과연 네덜란드 법원이 사용자의 행동에 대하여 당연히 적절한 책임을 묻게 될지는 의심스럽다. 더욱이 근로자의 행동을 통제하기 위하여 사설 조사관을 이용하는 것과 관련하여 네덜란드 판례법은 근로자가 근무시간 이후거나 회사 밖에 있었다 하여 사생활에 대한 정당한 기대가 항상 더 중요한 것으로 간주되지는 않는다고 보았다.[170]

세 번째로 사용자가 근로자를 통제할 자유로운 권리를 가지게 된다면 이는 이러한 권리의 남용으로 이어질 가능성이 높다. 근로자의 통제에 이용되는 수단에 관한 적절한 제한 조치가 없다면 사용자는 이러한 권리를 남용하게 되고 근로자는 어떠한 배상청구권도 가질 수 없게 된다. 근로자의 해고에 대한 보호가 약하다는 것을 감안하면 근로자의 통제에 대해 자유로운 권리를 갖는 것은 엄청난 영향을 가져올 수 있다. 예를 들어 Michael Rustad와 Sandra Paulsson은 사용자가 자유로운 통제권을 가지게 된다면 각종 퇴직급여나 혜택을 지급할 돈을 아끼면서 그럴듯한 명목으로 직원들을 해고하고자 하는 잘못된 동기를 제공할 수 있다는 점을 지적하였다.[171] 'TBG Insurance Services Corp. V. Superior Court' 사례는 이러한 점을 잘 보여준다.[172] 본 사례에서 Zieminski

169) See Phillips, supra note 31. 1993년 뉴욕주에서는 근로자가 근무시간이 아닌 시간에 회사 밖에서 합법적인 여가 활동에 참여한 것을 이유로 해고하는 것을 금하는 법률을 제정하였다.

170) Supreme Court 18 March 2003, NJ 2003/527 and Court of Appeal's Hertogenbosch 2 December 1992, NJ 1993/327; see also Hendrickx, supra note 86.

171) Rustad, supra note 2, at 45.

가 반복적으로 포르노사이트를 접속함을 TBG사가 인지한 후 고용계약을 해지하였다. 그러나 Zieminski는 본인이 이러한 사이트를 고의적으로 방문하지 않았음을 주장하였다. 즉 이러한 사이트들이 자동으로 팝업(pop up)했다고 주장한 것이다. 더욱이 Zieminski는 TBG사에 대한 소송을 제기하였는데, 회사가 실제로 해고한 이유는 본인의 스톡옵션 행사권이 발생하는 것을 막기 위해서였다는 것이다. 해고를 정당화할 만큼 심각하지 않은 사안이 해고의 실제 이유인 경우에도 사용자는 근로자를 해고할 이유를 찾기 위해 감시기술을 이용한다. 인터넷과 이메일 설비의 위법한 사용이 아닌 다른 이유가 해고의 실제 이유임을 근로자가 증명하기는 쉽지가 않다. 부당한 해고로 인한 부정적인 효과 이외에도 사생활 침해는 직원간 차별이라는 효과를 낳을 수 있다. 감시나 위치추적을 통하여 직원에 대해 수집한 정보를 바탕으로 회사는 근로자에게 주어지는 특정한 혜택을 배제할 수 있게 된다.

네 번째이자 마지막 이슈는 근로자 통제의 범위와 수단에 대한 주장이 갈수록 커져가고 점점 더 정교해져 간다는 점이다.[173] 예전의 기술에 적용되던 사생활 보호를 위한 법적 개념을 신기술에 적용하기 때문에 직원들을 통제할 사용자의 권한은 점점 더 증가하게 된다. 사용자의 통제권이 더 커 가면 근로자의 프라이버시권은 완전히 잠식되게 된다. 이런 면을 감안하여 David Phillips는 침해의 정도가 더 심한 감시기술의 이용과 정당화의 악순환을 언급하기도 하였다.[174] 그는 이러한 악순환을 다음과 같이 설명하였다:

예를 들어 사용자의 수색방침에 근로자가 명시적으로 동의하게 되면 사생활에 대한 정당한 기대는 줄어들거나 사라지게 된다고 법원은 판단하였다. 이런 경우 사용자는 이러한 동의를 당해 사업상 표준적인 관행으로 요구하게 된다. 이러한 표준적인 관행은 사업장 내 감시에 일반적으로 적용되는 사회의 규범으로 묵시적으로 받아들여지게 된다. 결국 감시에 대한 동의가 고용관계에서 암묵적으로 인정되게 된다.[175]

David Phillips는 자신의 주장에 대해 다음과 같이 결론을 지었다. 전체적으

172) *96 Cal. App. 4th 443 (Cal. App 2d Dist. 2002).*
173) 2004년 미국경영자협회의 보고서에 따르면 사용자의 60%가 근로자들의 이메일 송수신을 감시하는 소프트웨어를 사용하고 있다고 한다.
174) See Phillips, supra note 31, at 60.
175) Id.

로 보았을 때 사생활에 대한 법적 논쟁은 사용자의 근로자에 대한 권한을 증가시키는 방향으로 전개되어 왔다.[176] 기술의 발전이 프라이버시를 천천히 잠식해 왔기 때문에[177] 사용자와 근로자간 힘의 균형을 유지하고 또한 회복하기 위해서는 근로자에 대한 적절한 보호책이 만들어져야만 한다. 이러한 보호책은 기술적인 측면에서는 물론이고 필요한 법령을 제정함으로써 법적인 측면에서도 만들어져만 한다. 이는 근로자의 모든 행동을 감시함으로써 점점 더 강력해지고 있는 사용자의 권한에 대한 남용을 막기 위해서 필요한 것이다.

투고일: 2010. 6. 09 심사완료일: 2010. 6. 15 게재확정일: 2010. 6. 20

176) Id.

177) Leenes, supra note 121, at 48. 영상감시의 경우 감시가 행해지는 장소가 공공장소인지 여부가 매우 중요하다. 이메일 송수신이나 사적인 것이라고 명시된 인터넷 파일폴더에 대한 감시도 정당한 것으로 인정된다(최소한 미국에서는 사실이다). 또한 근로자에게 개인적 사용이 허락된 기기에 대해서는 근무시간외에도 감시가 허용된다. 가장 대표적인 예가 근로자와 근로자의 가족이 함께 사용하는 가정용 컴퓨터이다. 위치추적기술은 근무시간외는 물론 사업장 밖에까지 확장된다. 위치추적기술은 사용자에게 근로자의 실재 소재에 관한 정보를 24시간 제공할 수 있다. Id.

【 참 고 문 헌 】

1. 논문 및 단행본

Antoine Jacobs, Labour Law in the Netherlands, Kluwer Law International (2004).

Antoine Jacobs, Sociale rechten in Amerika, Utrecht: LEMMA BV, 212 (2003).

Dan Long, The Electronic Workplace, Modrall, Sperling, Roehl, Harris & Sisk, P.A., June 3, 2002.

David J. Phillips, Privacy and Data Protection in the Workplace: the U.S. Case, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, 42 (2005).

Gellman, R., A General Survey of Video Surveillance Law in the United States, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, Den Haag: T.C.M. Asser press (2005).

Jay P. Kesan, Cyber-Working or Cyber-Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace, 54 Fla. Law Rev. 289, 319 (2002).

J.E. Davidson, Reconciling the Tension Between Employer Liability and Employee Privacy, 8 Geo. Mason U. Civ. Rts. L.J. 145, 147 (1997).

Jill Yung, Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should do About It, 36 Seton Hall L. Rev. 163, 192 (2005).

Karen Eltis, The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Case law in Canada and

Israel: Should Others Follow Suit?, 24 Comp. Lab. L. & Pol'y J. 487 (2003).

Kenneth A. Kovach, The Balance Between Employee Privacy And Employer Interests, 105 Business and Society Review 289, 295 (2000).

M. Ishman, 'Comment', Computer Crimes and the Respondeat Superior Doctrine: Employers Beware, 6 B.U. J. Sci. & Tech. L. 6 (2000).

Mark Sullivan, Wired, Arnold Vetoes Privacy Bill, Sept. 30, 2004.

Matthew T. Bodie, The Potential for State Labor Law: The New York Greengrocer Code of Conduct, 21 Hofstra Lab. & Emp. L.J. 183, 185 (2003).

Michael Rustad & Sandra R. Paulsson, Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshops: Insights from Europe, 7 U. Pa. J. Lab. & Emp. L. 829 (2005).

P. Blok, Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht, Boom Juridische Uitgevers (2002).

Peter Blackman & Barbara Franklin, Blocking Big Brother: Proposed Law Limits Employer's Right to Snoop, N.Y. L. J., at 5 (1993).

Peter Caldwell, GPS Technology in Cellular Telephones: Does Florida's Constitutional Privacy Protect Against Electronic Locating Devices?, 11 J. Tech. L. & Pol'y 39, 44 (2006).

R. Blanpain & Michelle Colucci, The Impact of the Internet and New Technologies on the Workplace. A Legal Analysis from a Comparative Point of View, The Hague: Kluwer (2002).

R. Blanpain, On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work, The Hague/ London/New York: Kluwer (2002).

Robert Fragale Filhot & Mark Jeffery, Information Technology and Workers' Privacy: Notice and Consent, A Comparative Study: Part III: Recurring Questions of Comparative Law, 23 Comp. Lab. L. &

Pol'y J. 471, 557-558 (2002).

R. Gellman, A General Survey of Video Surveillance Law in the United States, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series 7, Den Haag: T.C.M. Asser Press (2005).

Roberto Fragale Filhot and Joaquim Leonel de Rezende Alvim, Information Technology and Workers' Privacy: Old and New Paradigms, 23 Comp. Lab. L. & Pol'y J 527, 527-532 (Winter 2002).

Ronald Leenes & Bert-Jaap Koops, 'Code' and Privacy: Or How Technology is Slowly Eroding Privacy, The Hague, 43 (Asscher Press 2005).

2. 인터넷 기타 자료

American Management Association, Internet Monitoring, http://www.amanet.org/research/pdfs/IM 2004 Summary.pdf

Earnest & Young, ICT Borometer, http://www.ict-barometer.nl/rapporten.php

Electronic Privacy Information Center(EPIC), Workplace Privacy, http://www.epic.org/privacy/workplace

European Court of Human Rights Portal, www.echr.coe.int

<국문요약>

정보통신기술과 사용자－근로자간의 역학관계
－정보통신기술에 의한 근로자 감시 및 근로자의 위치추적에 있어서 사업장 내 프라이버시에 대한 미국과 네덜란드의 비교법적 관점의 연구－

Colette Cuijpers · 이재용

정보통신기술의 눈부신 발전은 전통적인 근로관계에도 많은 혁신을 가져왔다. 사업장에서는 컴퓨터 등 정보기기가 보급되고 인터넷, 이메일 등의 사용이 보편화되면서 근로제공에 있어 시간적, 공간적 제약은 더 이상 문제되지 않게 되었다. 기업들의 업무능률과 생산성이 과거와 비교할 수 없을 만큼 형상되었음은 물론이다.

그러나 이러한 정보통신기술의 발전은 동시에 사용자와 근로자 모두에게 새로운 위협으로 작용하고 있다. 사용자의 입장에서는 인터넷과 이메일을 통해 기업의 중요한 영업비밀이 누설되고 있는 것은 아닌지 걱정하게 되었고, 근로자들은 정보통신기술이 사업장 내에서는 물론 사업장 밖에서까지 근로자를 감시하고 개인의 프라이버시를 침해하는 도구로 이용되는 상황에 직면하게 되었다.

본 논문에서는 정보통신기술이 갖는 이러한 이중적 성격에 착안하여 정보통신기술이 사용자와 근로자간의 역학관계에 어떤 영향을 미쳐왔는지, 또 이러한 역학관계의 변동을 규율하기 위해서는 어떤 수준의 규제가 적절한지 등을 규명하고자 하였다. 이를 위하여 프라이버시에 관한 미국과 네덜란드의 상반된 접근방식을 비교 · 검토하였다.

전통적으로 미국에서는 프라이버시가 시장원리에 의하여 일종의 재산권의 입장에서 다루어진데 반해 네덜란드에서는 기본적인 인권의 문제로 다루어져 왔고 이러한 차이는 노동법의 영역에서도 그대로 나타나 있다. 따라서 이러한 비교법적 연구를 통해 궁극적으로는 사용자에 의한 인터넷과 이메일에 대한 감시

나 위치추적 등의 허용여부와 허용정도, 근로자의 프라이버시를 보호하기 위해서는 어떤 대책을 강구해야 하는지 등에 대한 일반적인 결론을 도출할 수 있을 것으로 생각한다.

핵심어 : 정보통신기술, 프라이버시, 전자감시, 인터넷과 이메일 감시, 사생활의 침해

<Abstract>

ICT and Employer-Employee Power Dynamics
-A Comparative Perspective of United States' and Netherland's Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning-

Collette Cuijpers
Professor
Tilburg University Law School

Lee, Jae-Yong
Adjunctive Professor
Department of Law
Sookmyung Women's University

The dazzling progress in information and computer technology has brought many remarkable changes in the traditional employment relationship. Now when information equipment like computers has become common in workplaces and the use of the Internet and emails has been popularized, labor can be provided without limitations in time and space. As a result, companies are enjoying work efficiency and productivity higher than ever.

On the other hand, however, the advance of information and computer technology is working as a new threat to both employers and employees. Employers worry whether crucial trade secrets may leak out through the Internet and emails, and employees are faced with the situation that such technologies may be used to monitor the employees even outside the workplace and to intrude their privacy.

Taking note of such a dual nature of information communication

technology, this study purposed to examine how information and computer technology has affected the dynamic relation between employers and employees, and what level of regulations is appropriate for regulating the change of the dynamic relation. For this purpose, we compared the contrastive approaches to privacy in the U.S. and the Netherlands.

While the U.S. has dealt with privacy as a kind of property right based on market principles, the Netherlands has handled it as a basic human right. This difference is reflected clearly in their labor laws. Accordingly, through research from the viewpoint of comparative law, we expect to draw general conclusions on whether to allow employers' monitoring or position tracking over the Internet and emails, the extent of the allowance, measures to be prepared for protecting employees' privacy, etc.

Key Words : Information and computer technology, privacy, electronic monitoring(surveillance), the Internet and email monitoring, invasion of privacy